





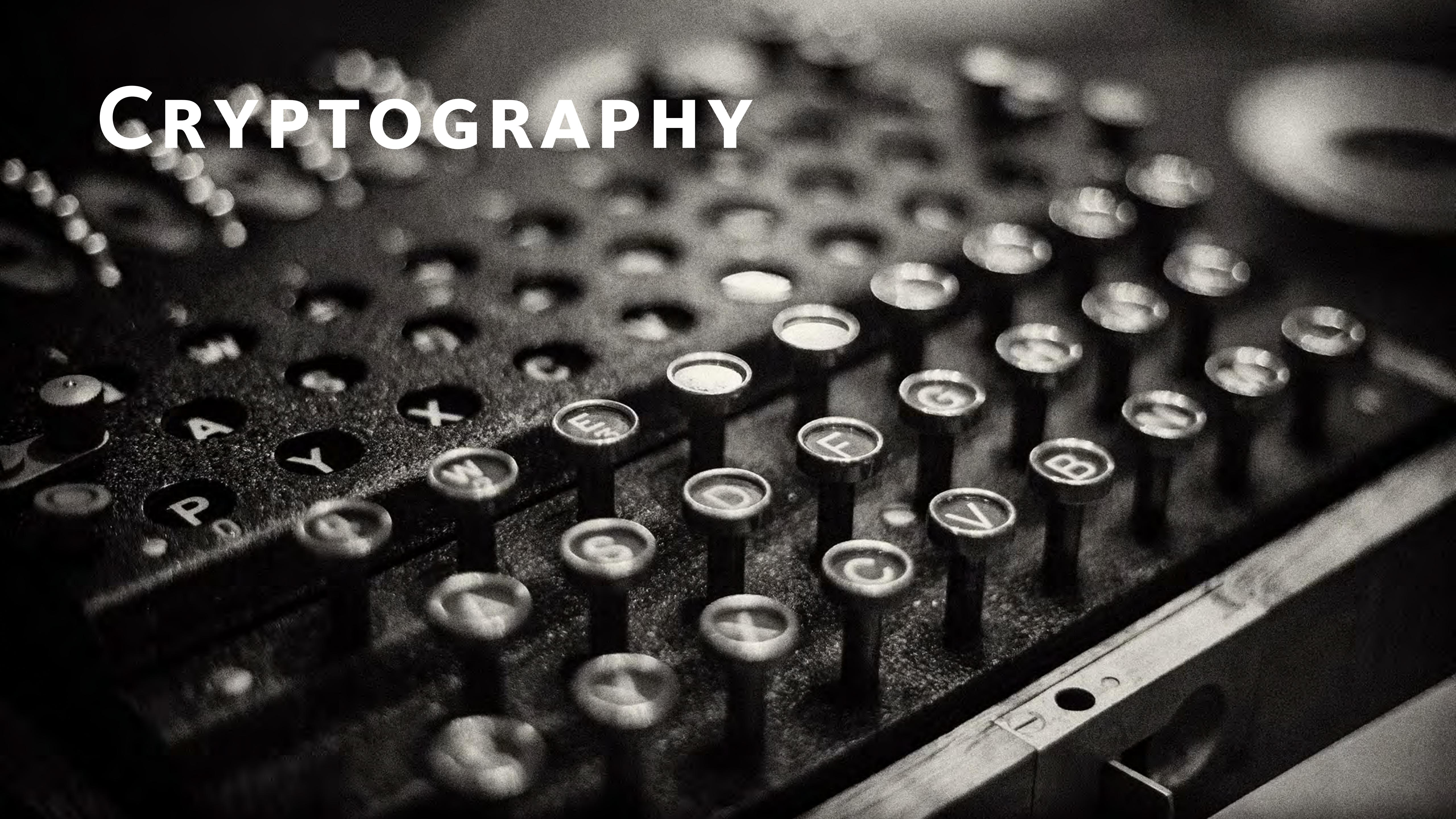
UNIVERSITY OF  
**OXFORD**



# CERTIFICATES

## How DO THEY WORK?

# CRYPTOGRAPHY



# SYMMETRIC KEYS



Bob



ALICE

# SYMMETRIC KEYS



# SYMMETRIC KEYS



# SYMMETRIC KEYS

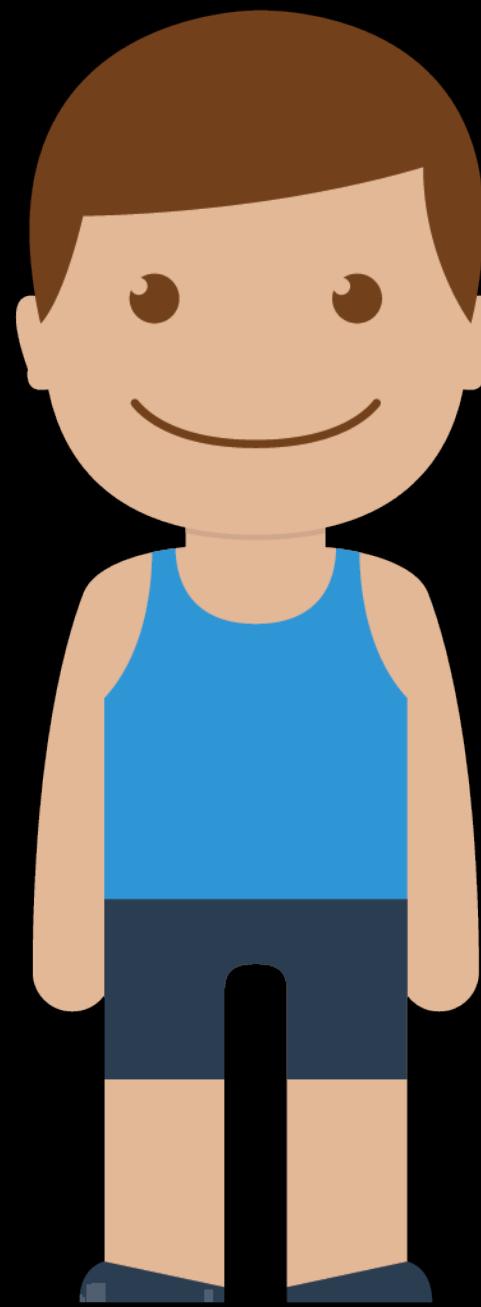


# SECURE KEY EXCHANGE

- Meet in person for secure key exchange
  - Impractical for many people / large groups
  - Often impossible
- Secure cryptographic key exchange over a public channel
  - Extra complexity and overheads
  - Example: Diffie-Helman key exchange



# PUBLIC KEY CRYPTOGRAPHY – IDEA



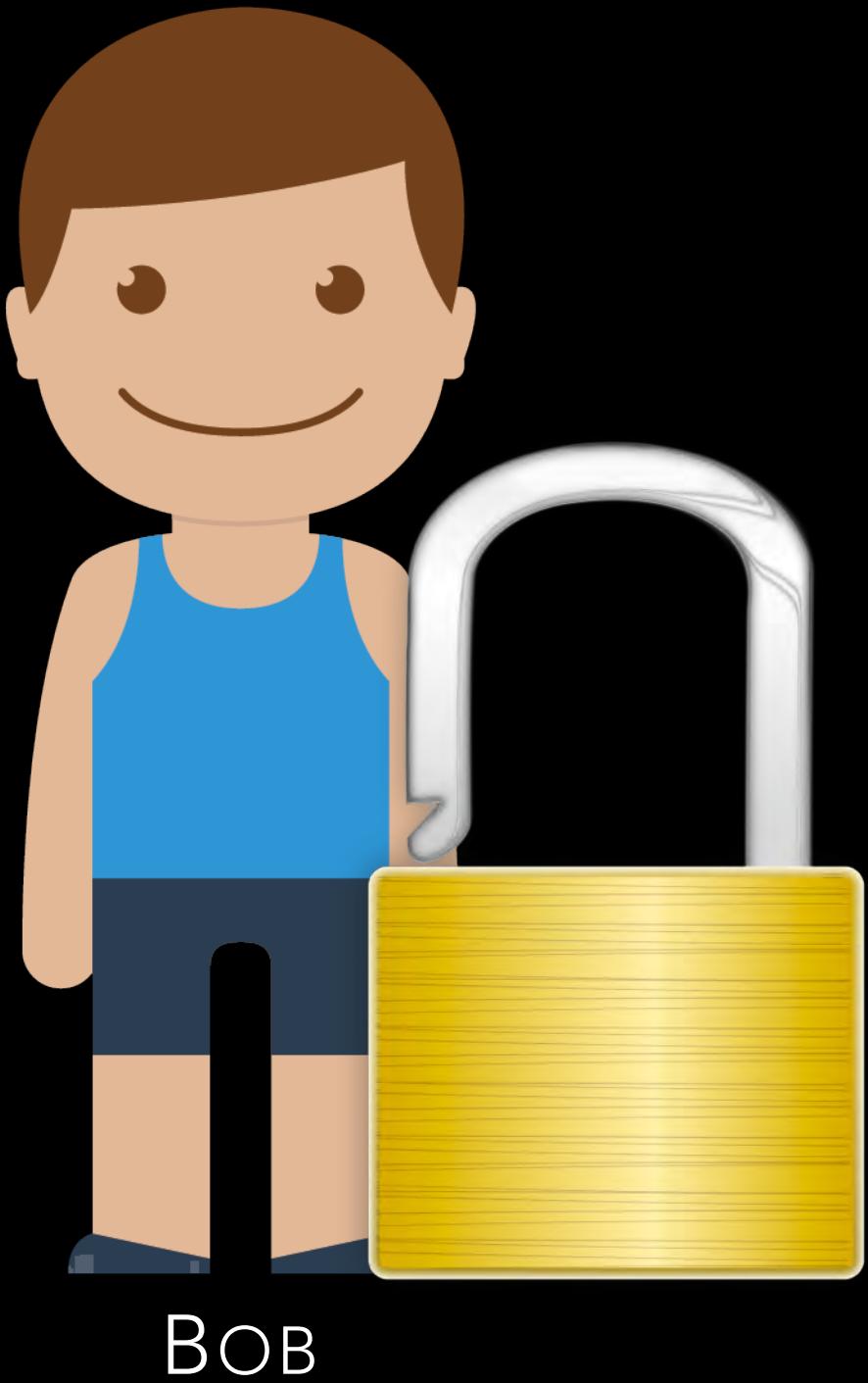
BOB

1.Lock: encryption key  
Key: decryption key

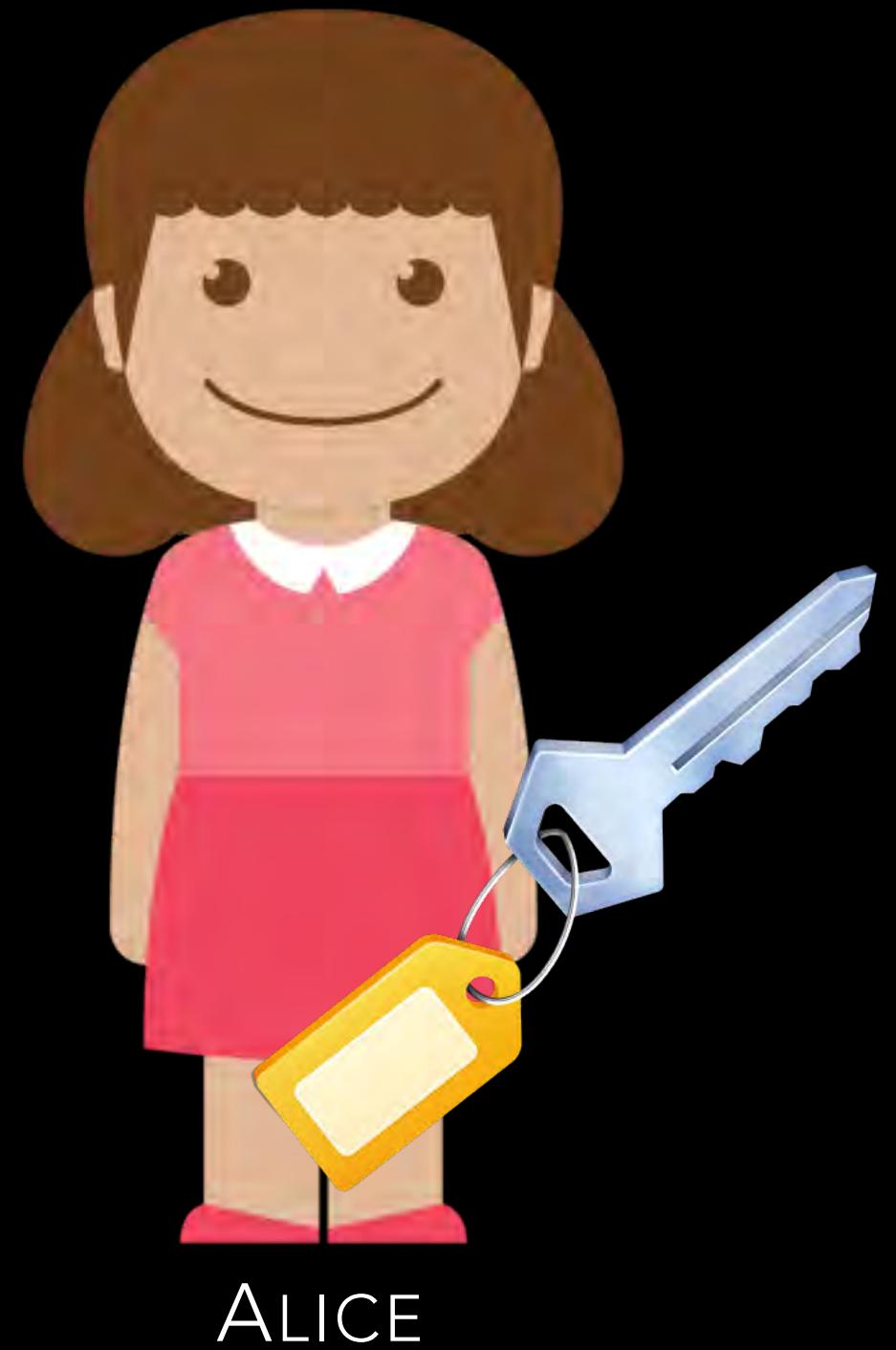


ALICE

# PUBLIC KEY CRYPTOGRAPHY – IDEA



- 1.Lock: encryption key  
Key: decryption key
- 2.Encryption key may be shared in public  
as it can only perform a one-way function



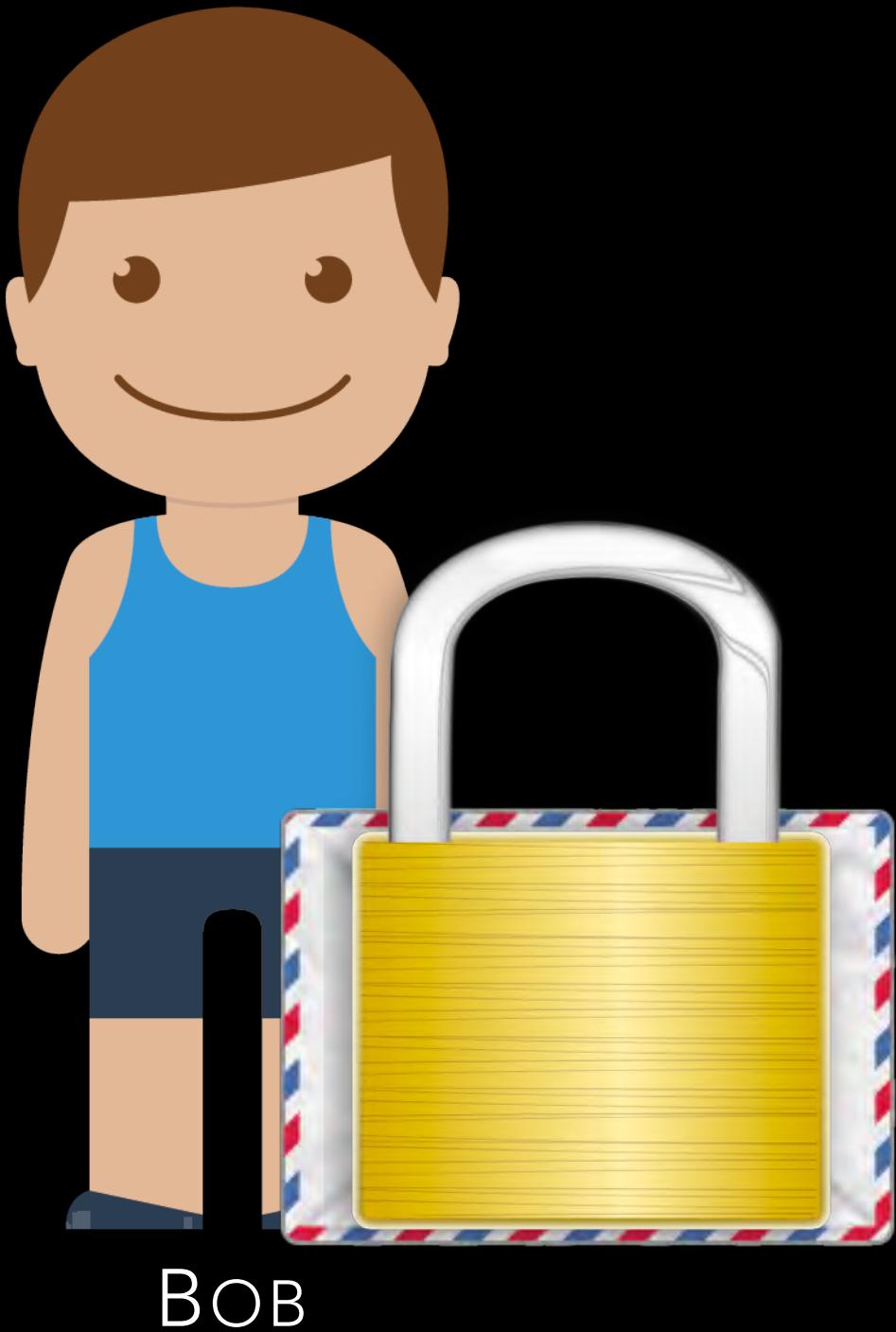
# PUBLIC KEY CRYPTOGRAPHY – IDEA



- 1.Lock: encryption key  
Key: decryption key
- 2.Encryption key may be shared in public  
as it can only perform a one-way function



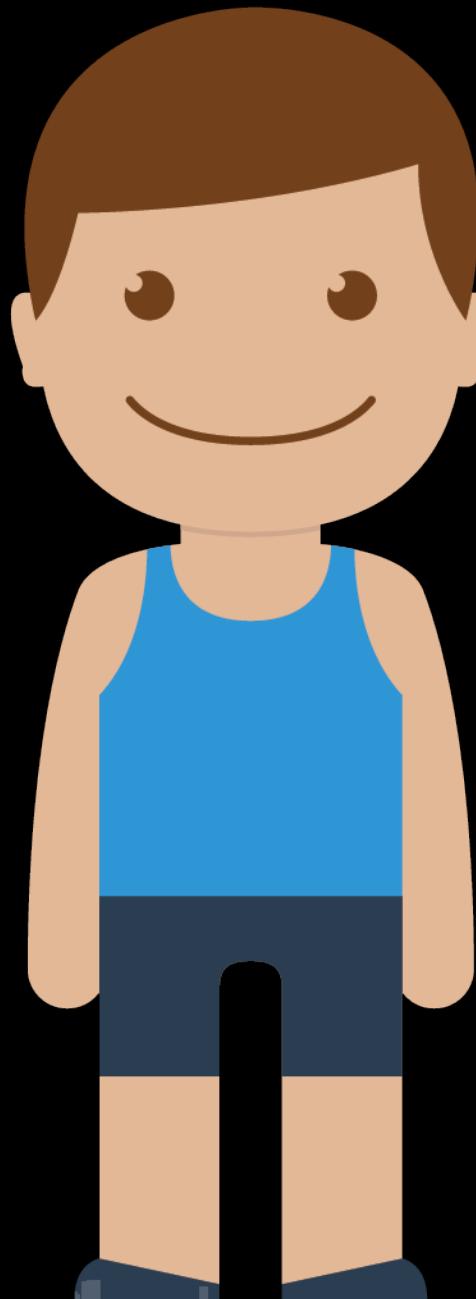
# PUBLIC KEY CRYPTOGRAPHY – IDEA



- 1.Lock: encryption key  
Key: decryption key
- 2.Encryption key may be shared in public  
as it can only perform a one-way function



# PUBLIC KEY CRYPTOGRAPHY – IDEA



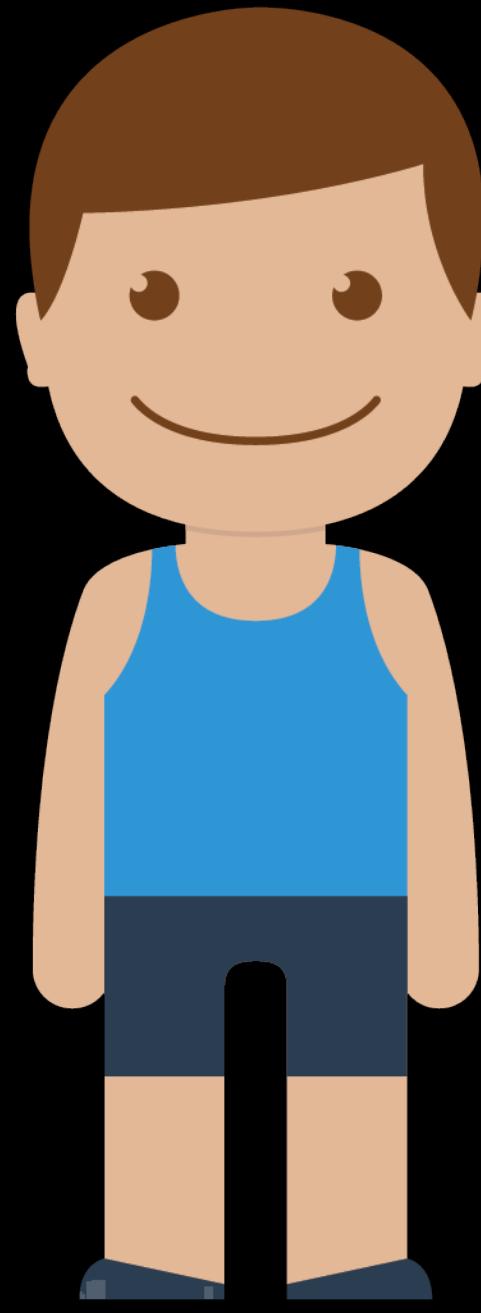
BOB

- 1.Lock: encryption key  
Key: decryption key
- 2.Encryption key may be shared in public  
as it can only perform a one-way function



ALICE

# PUBLIC KEY CRYPTOGRAPHY – IDEA

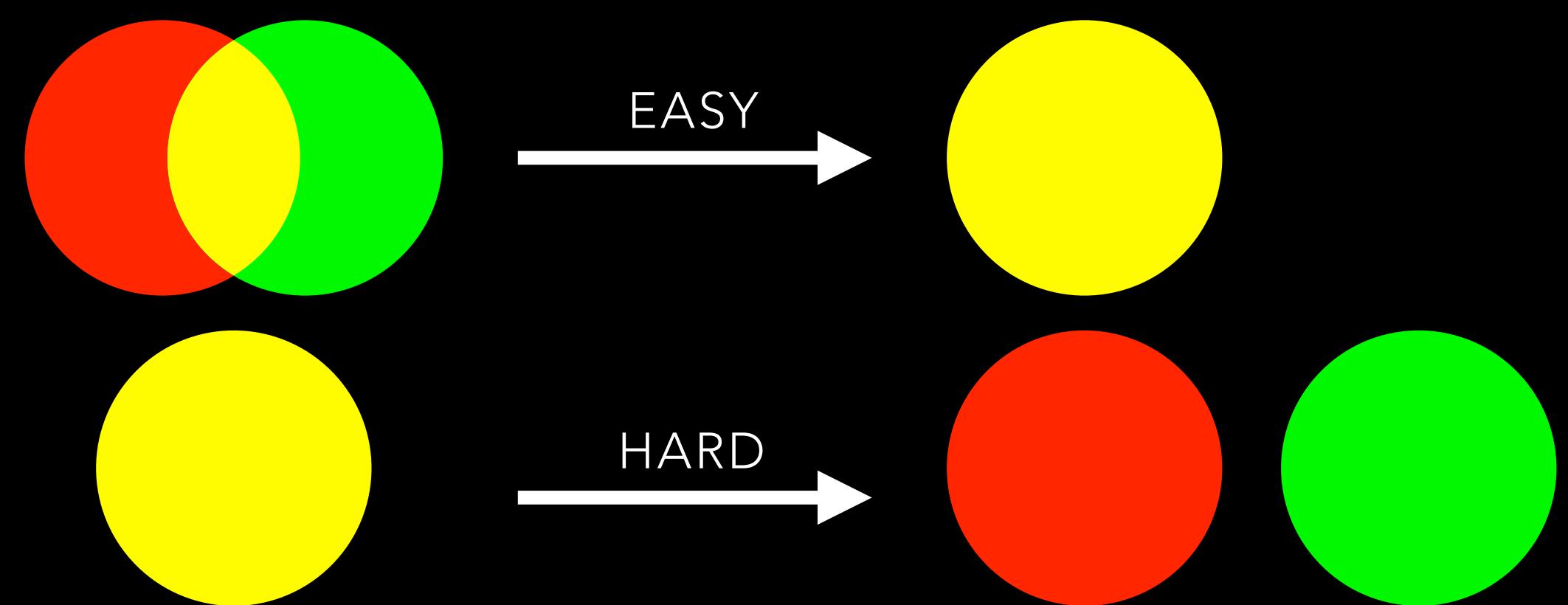
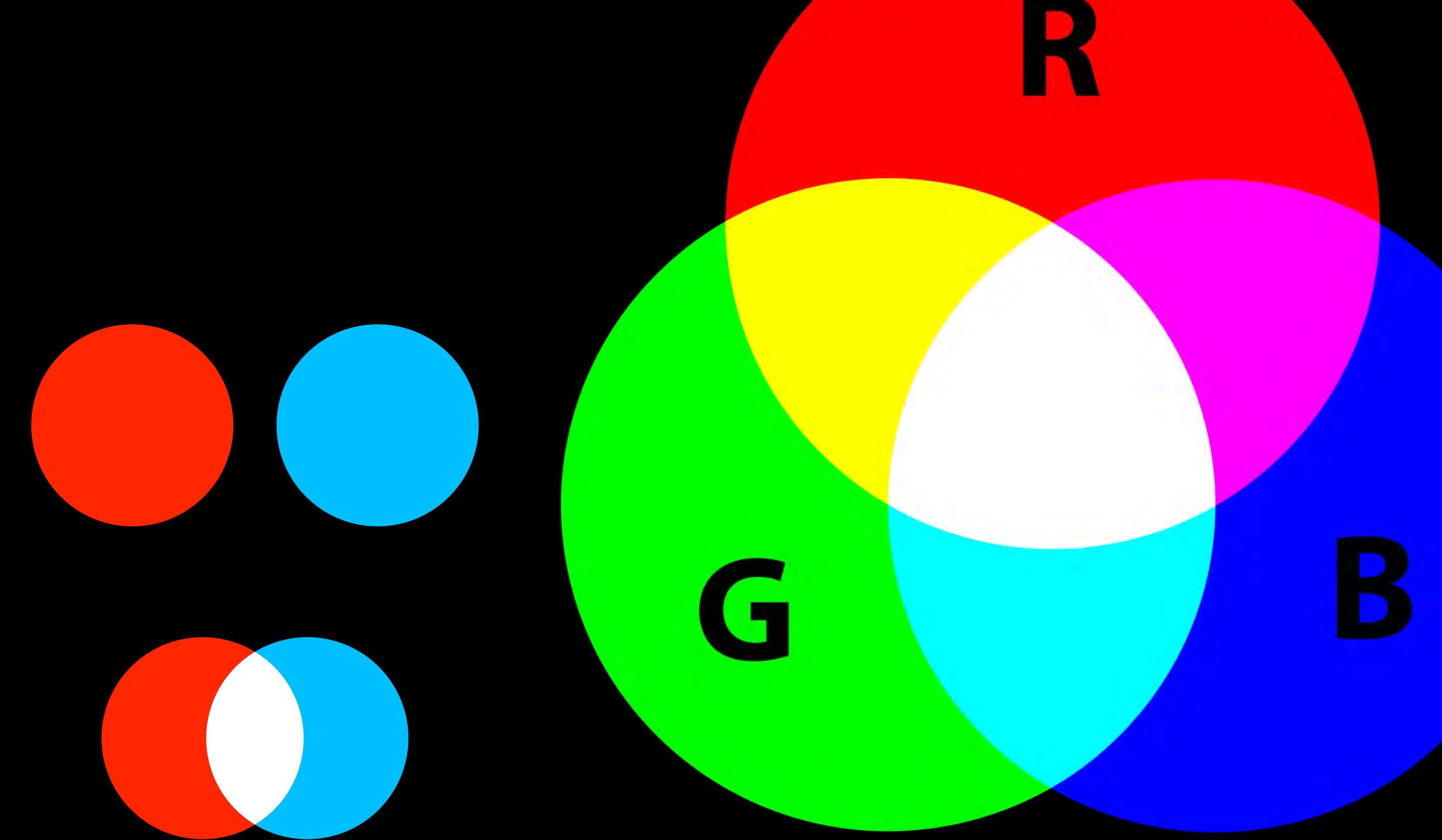


- 1.Lock: encryption key  
Key: decryption key
- 2.Encryption key may be shared in public  
as it can only perform a one-way function
- 3.Decryption key performs the inverse  
(or undo) operation which was applied  
by the encryption key.

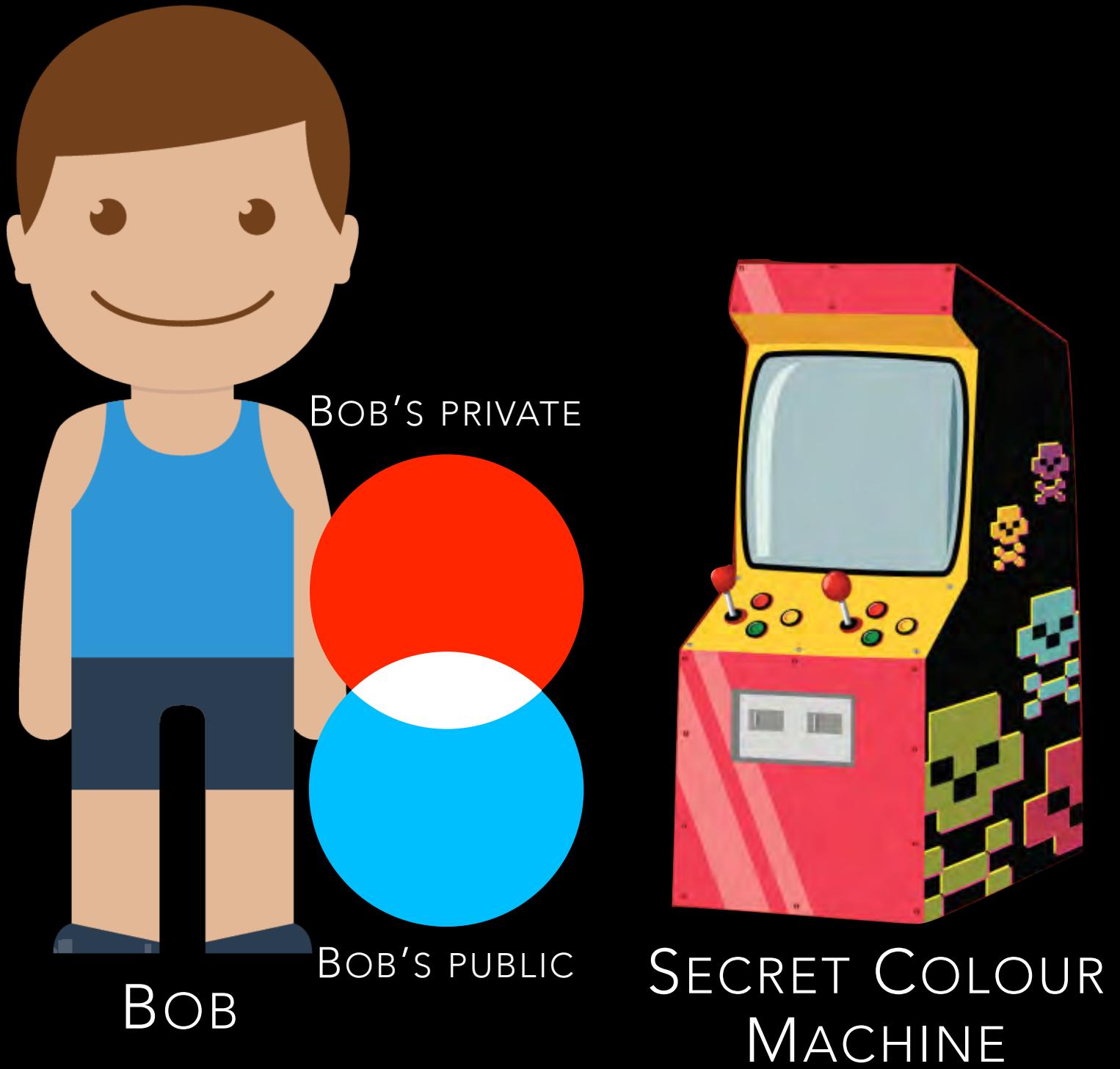


# ASSUMPTIONS

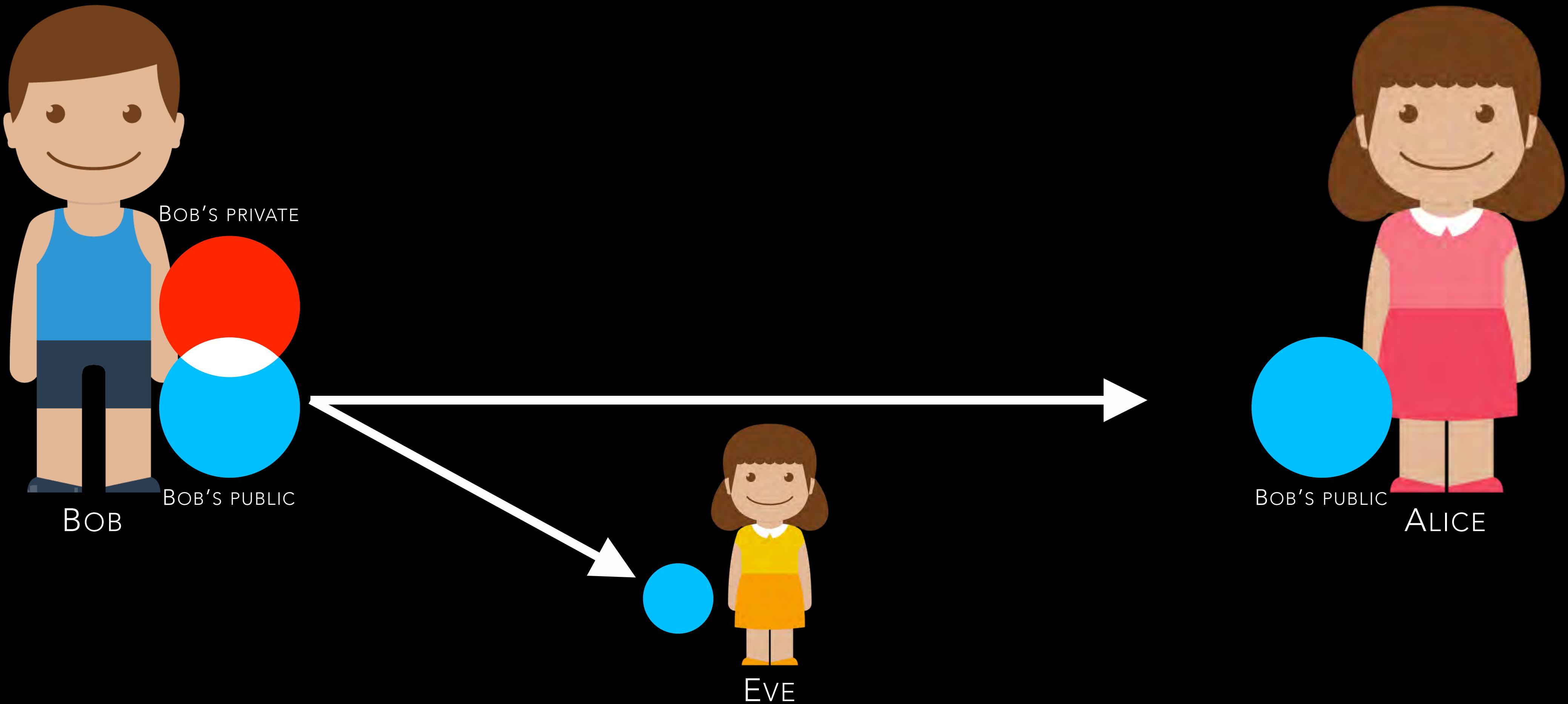
1. The inverse of an additive colour is called complementary colour.
2. Adding the complementary colour to a colour produces white (undoes the effect of the colour)
3. Mixing colours is a one-way function as mixing is fast, but slow to undo.



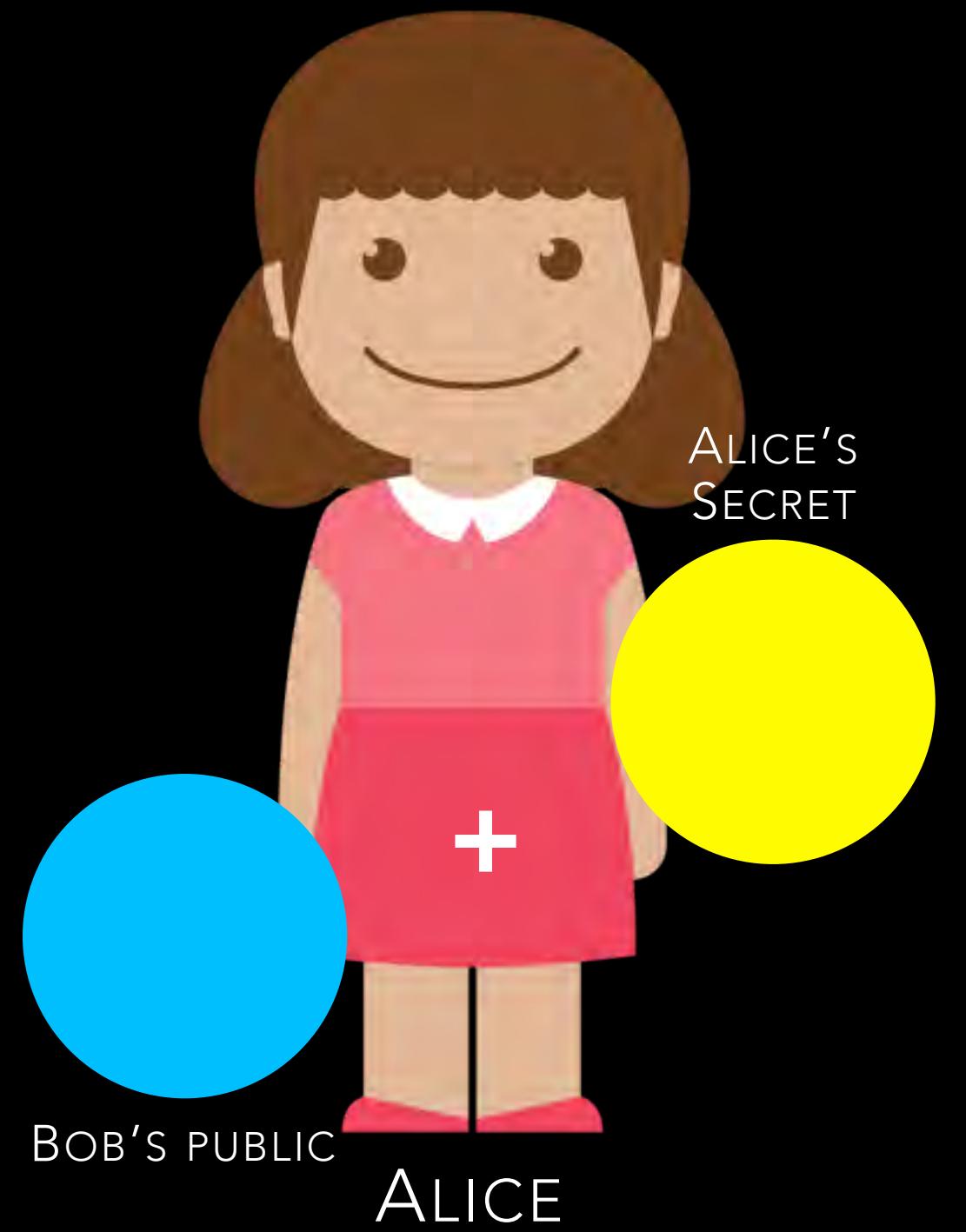
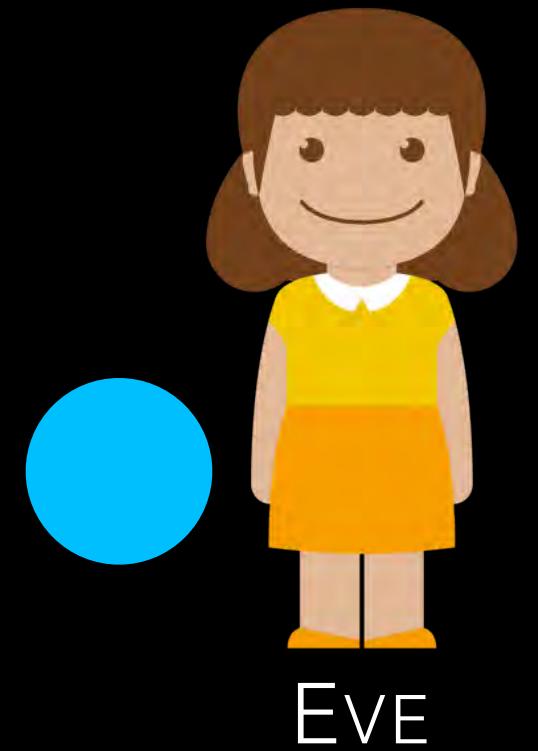
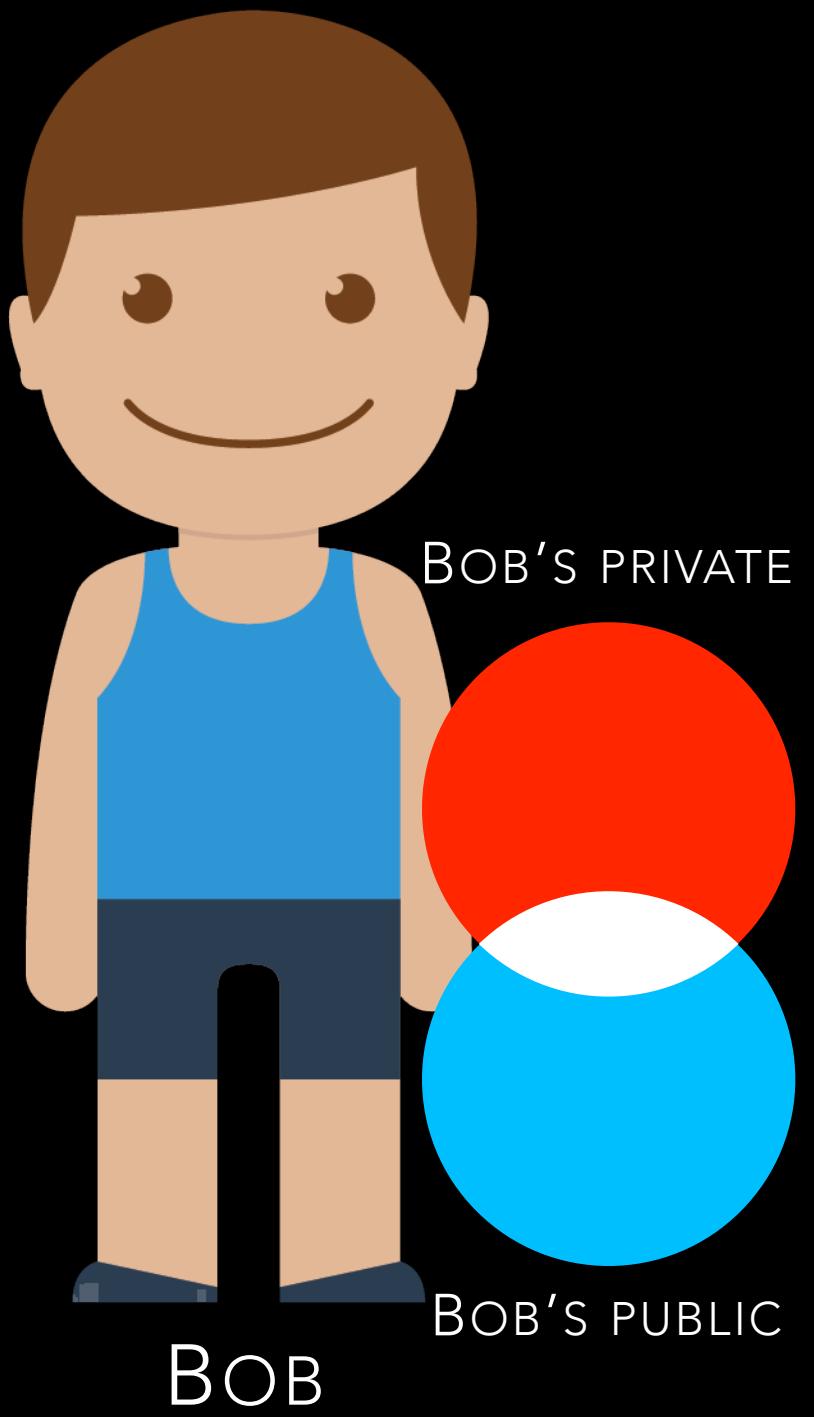
# PUBLIC KEY CRYPTOGRAPHY – ENCRYPTION



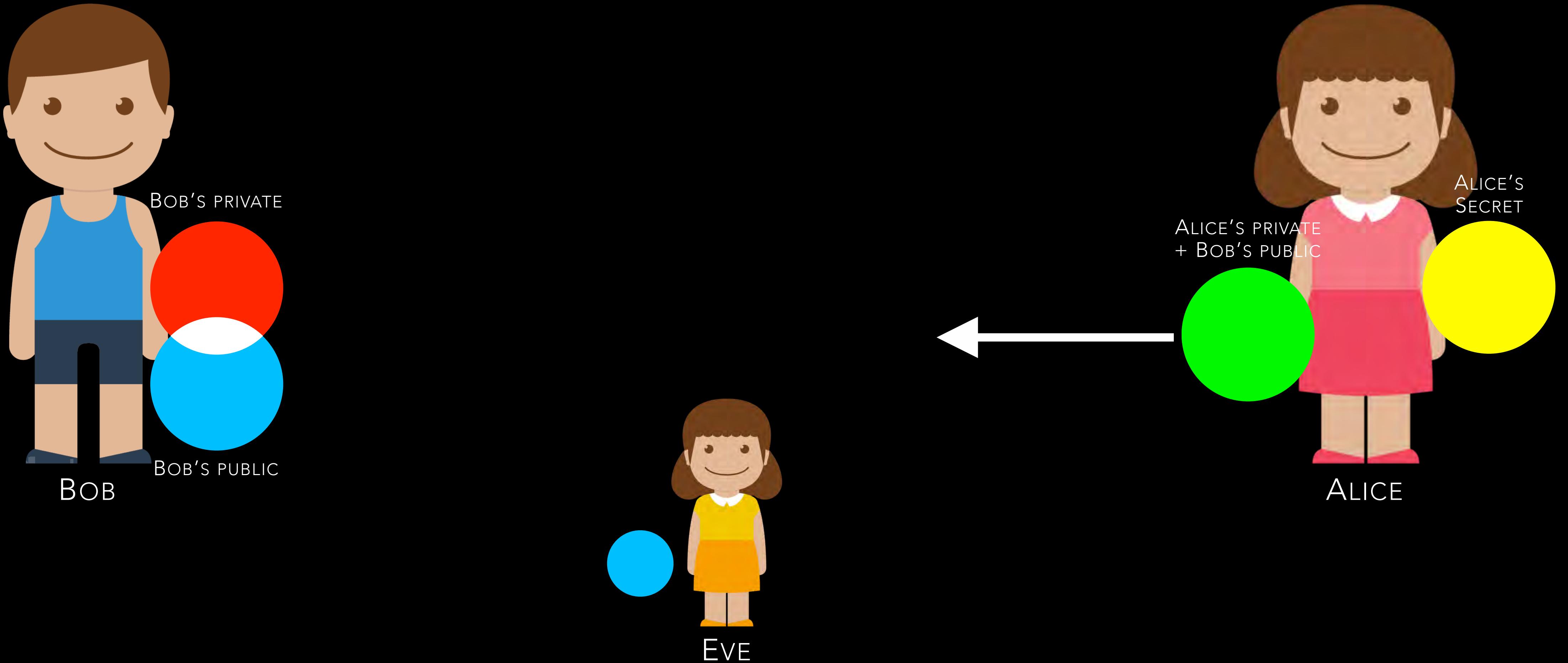
# PUBLIC KEY CRYPTOGRAPHY – ENCRYPTION



# PUBLIC KEY CRYPTOGRAPHY – ENCRYPTION



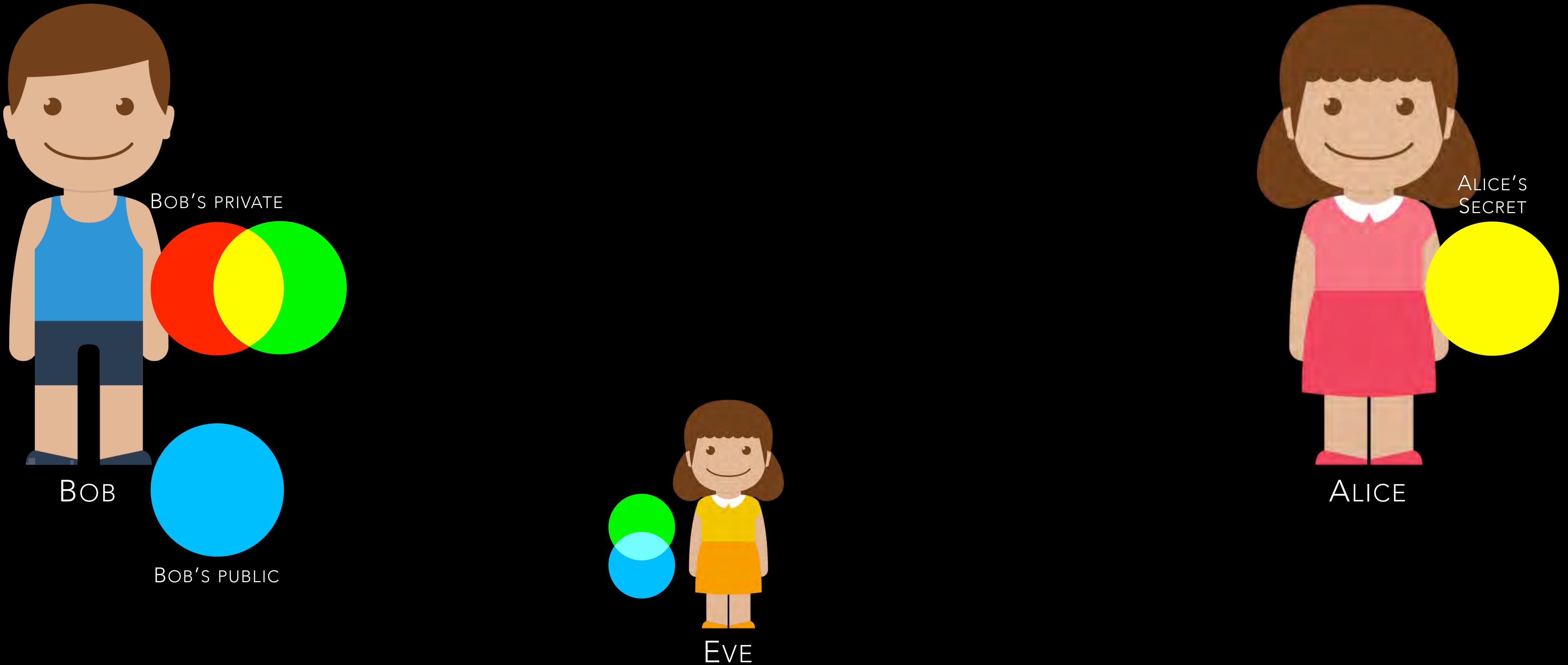
# PUBLIC KEY CRYPTOGRAPHY – ENCRYPTION



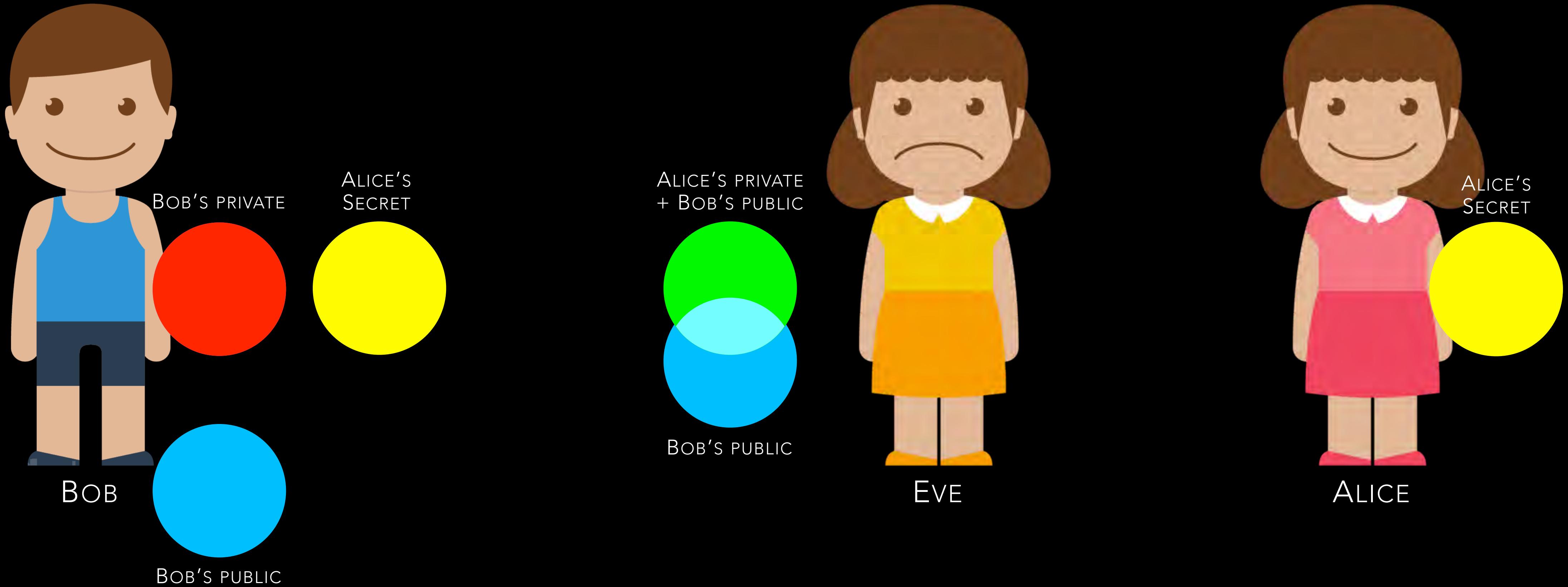
# PUBLIC KEY CRYPTOGRAPHY – ENCRYPTION

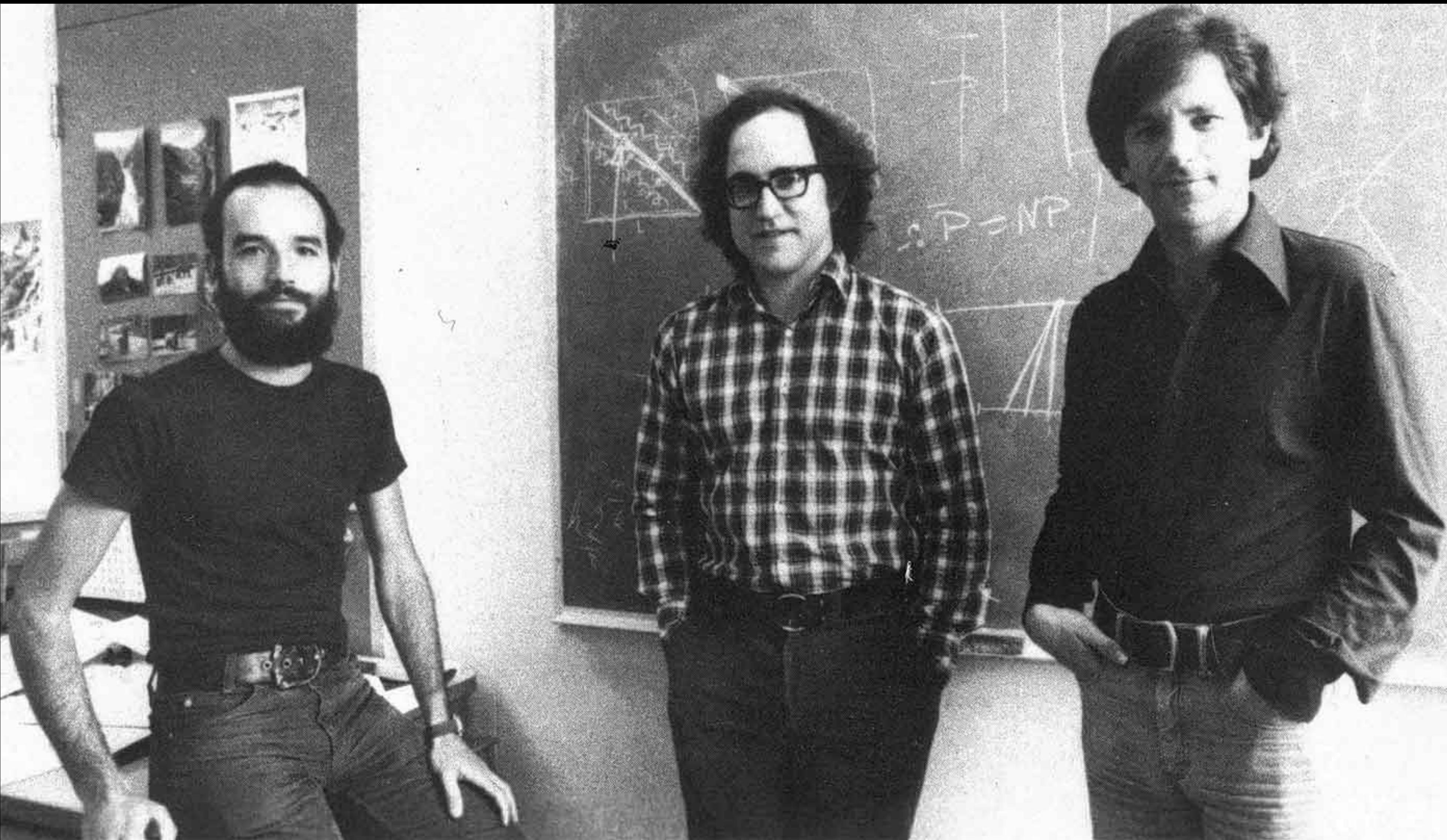


# PUBLIC KEY CRYPTOGRAPHY – ENCRYPTION



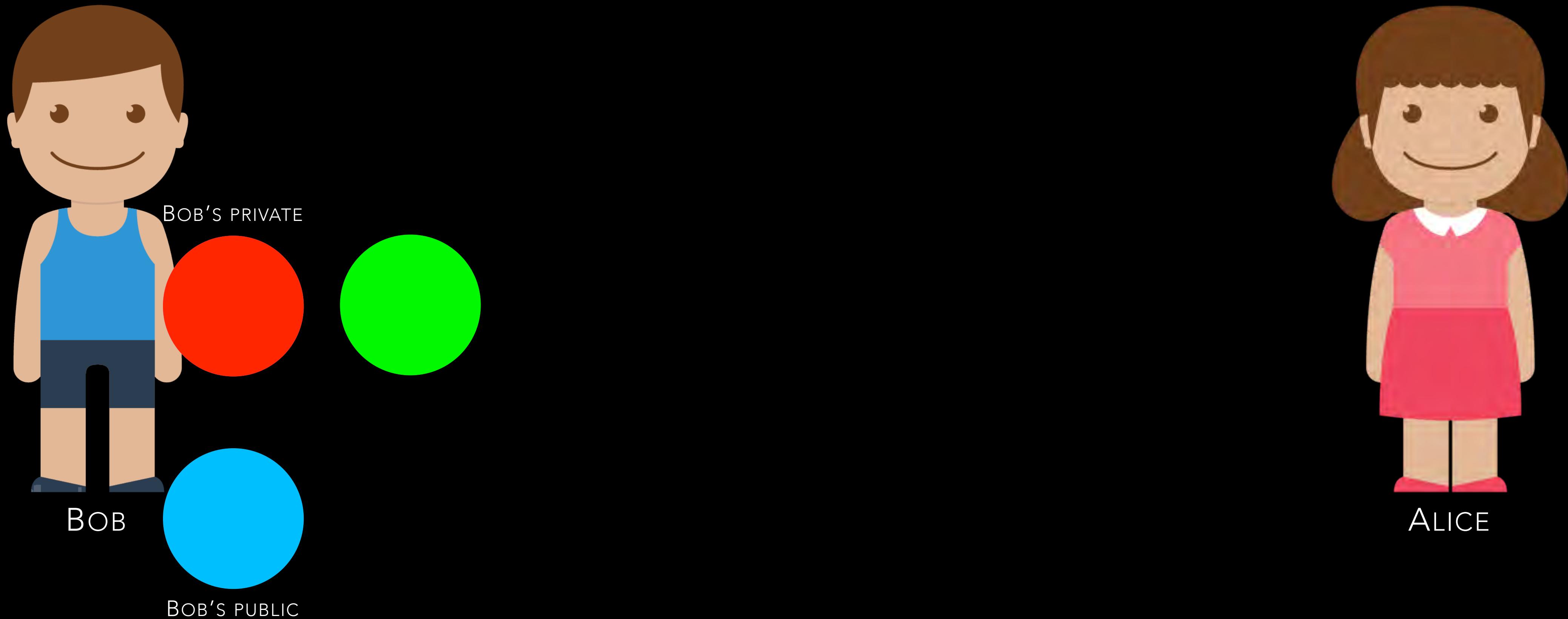
# PUBLIC KEY CRYPTOGRAPHY – ENCRYPTION



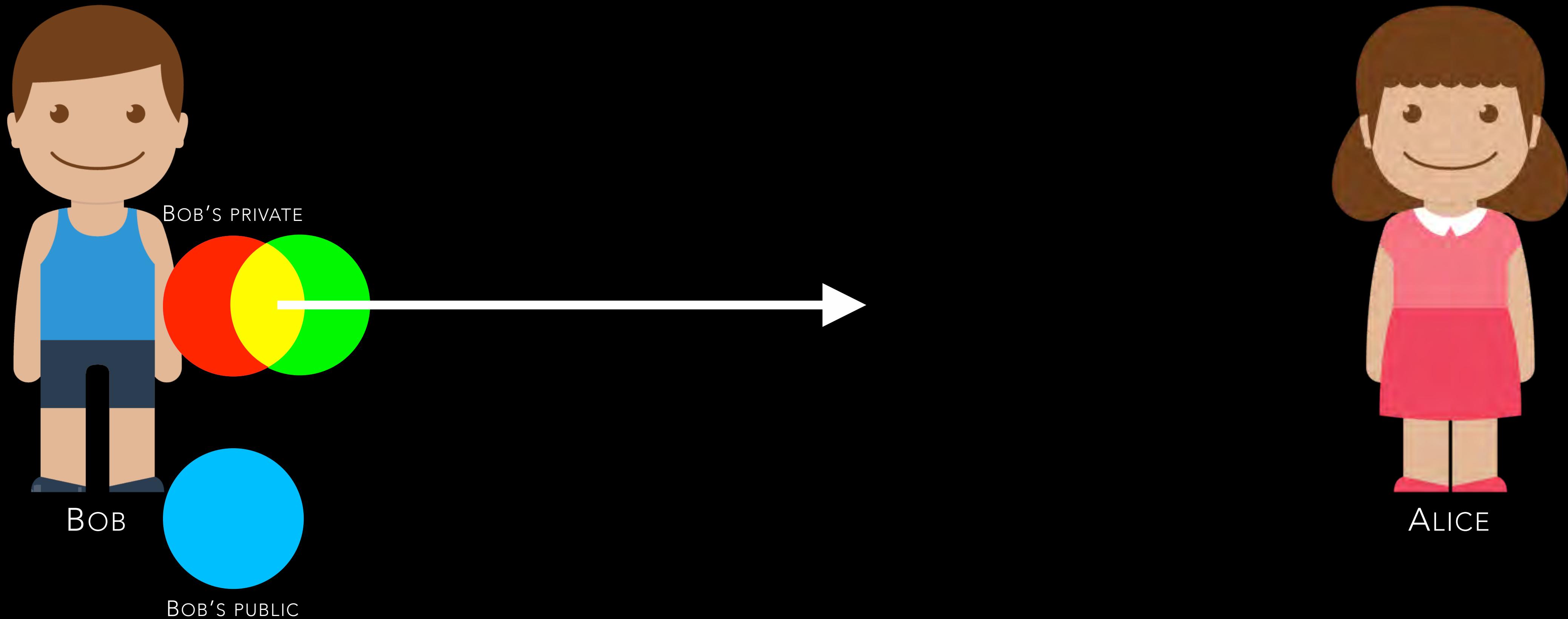


**Ron Rivest, Adi Shamir, and Leonard Adleman** – the inventors of RSA (1977)

# PUBLIC KEY CRYPTOGRAPHY – SIGNATURES



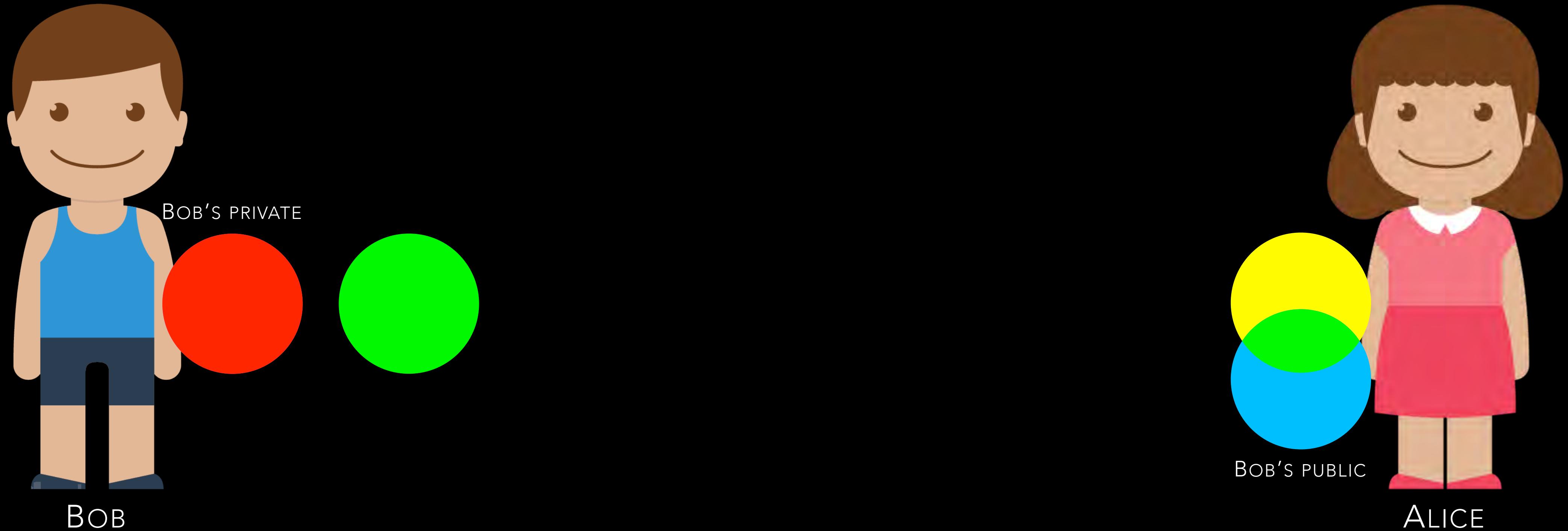
# PUBLIC KEY CRYPTOGRAPHY – SIGNATURES



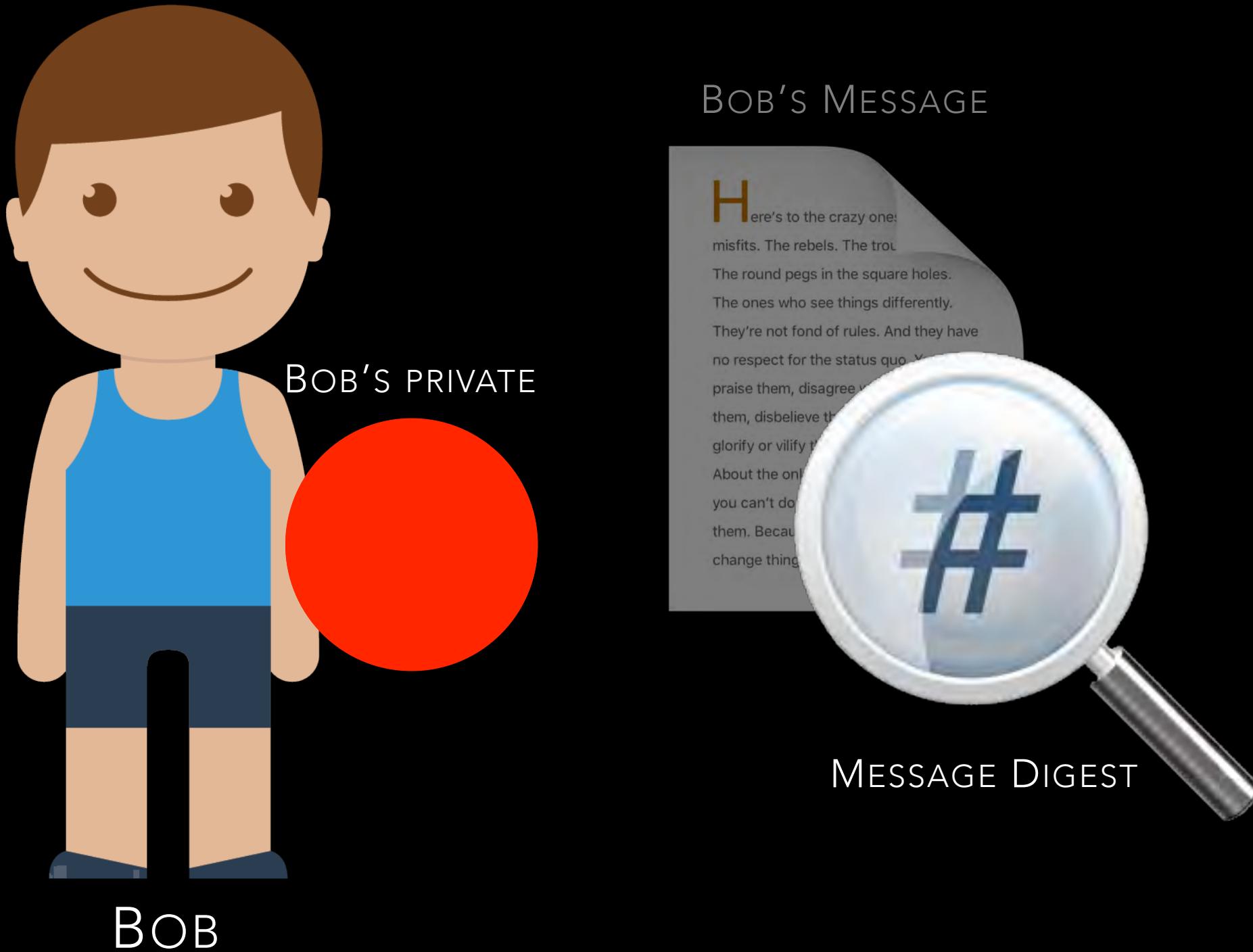
# PUBLIC KEY CRYPTOGRAPHY – SIGNATURES



# PUBLIC KEY CRYPTOGRAPHY – SIGNATURES

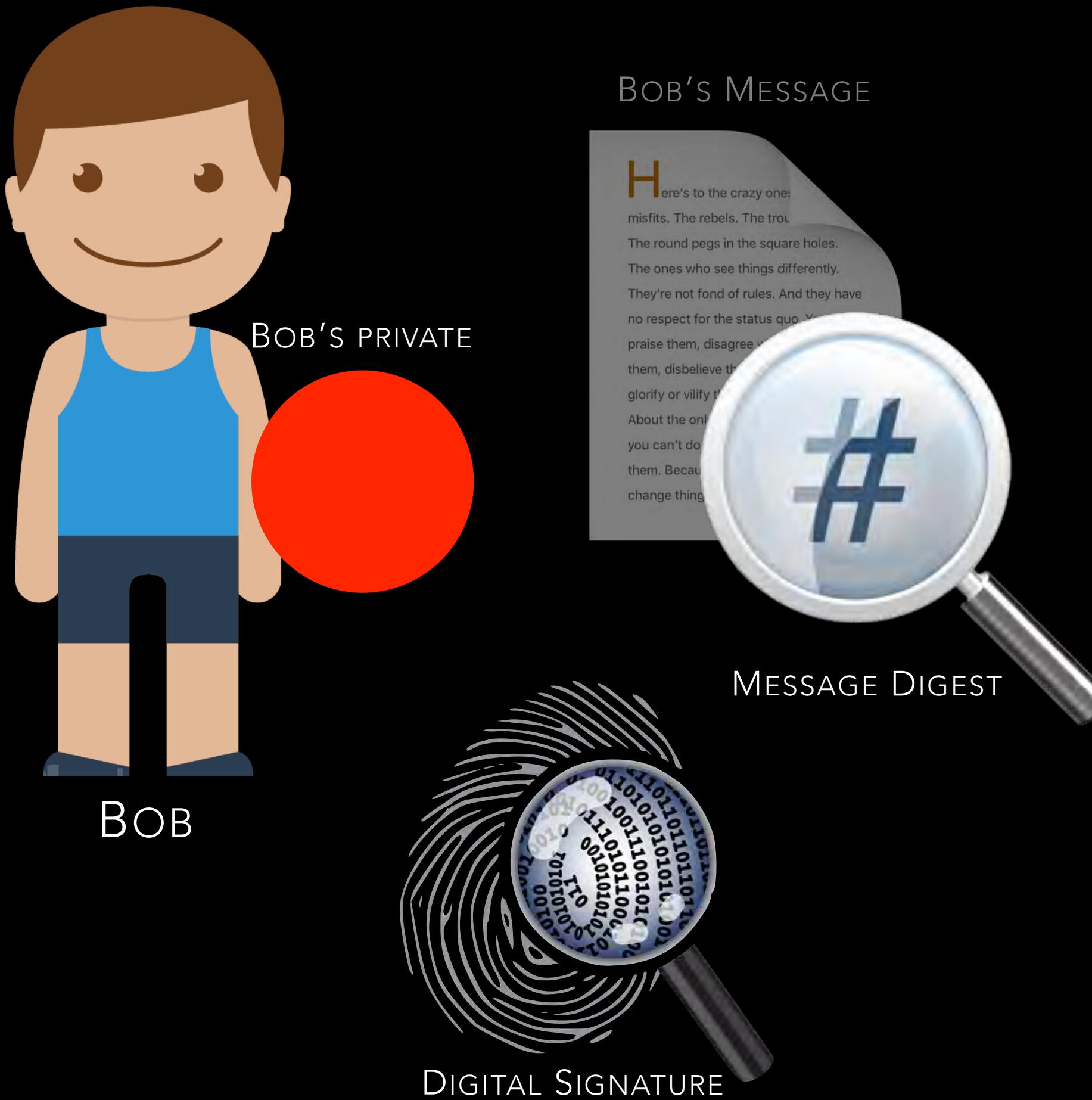


# PUBLIC KEY CRYPTOGRAPHY – SIGNATURES



1. Bob computes the message hash to create the message digest.

# PUBLIC KEY CRYPTOGRAPHY – SIGNATURES

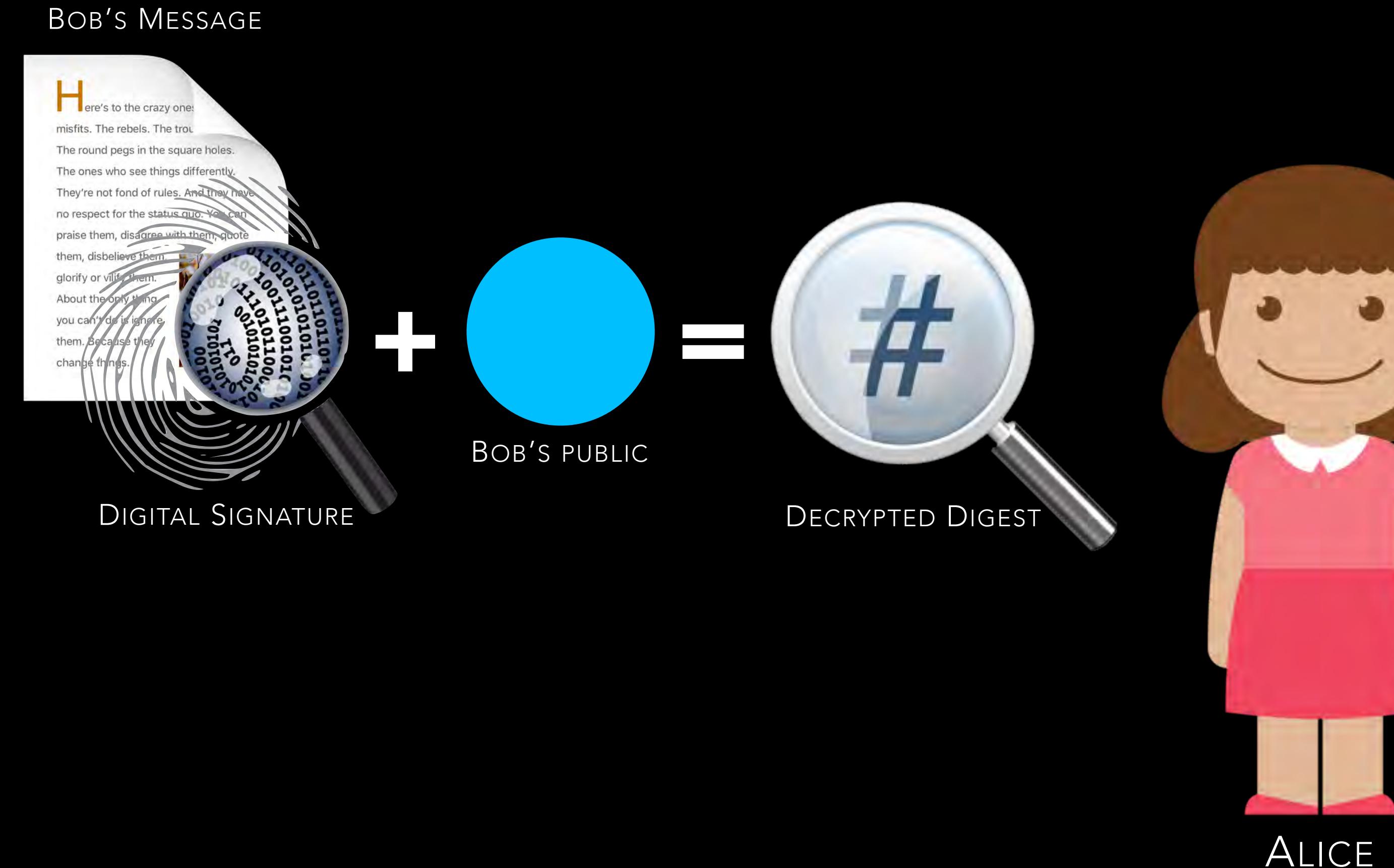


1. Bob computes the message hash to create the message digest.
2. Bob encrypts the message digest with his private key to create a digital signature.

# PUBLIC KEY CRYPTOGRAPHY – SIGNATURES

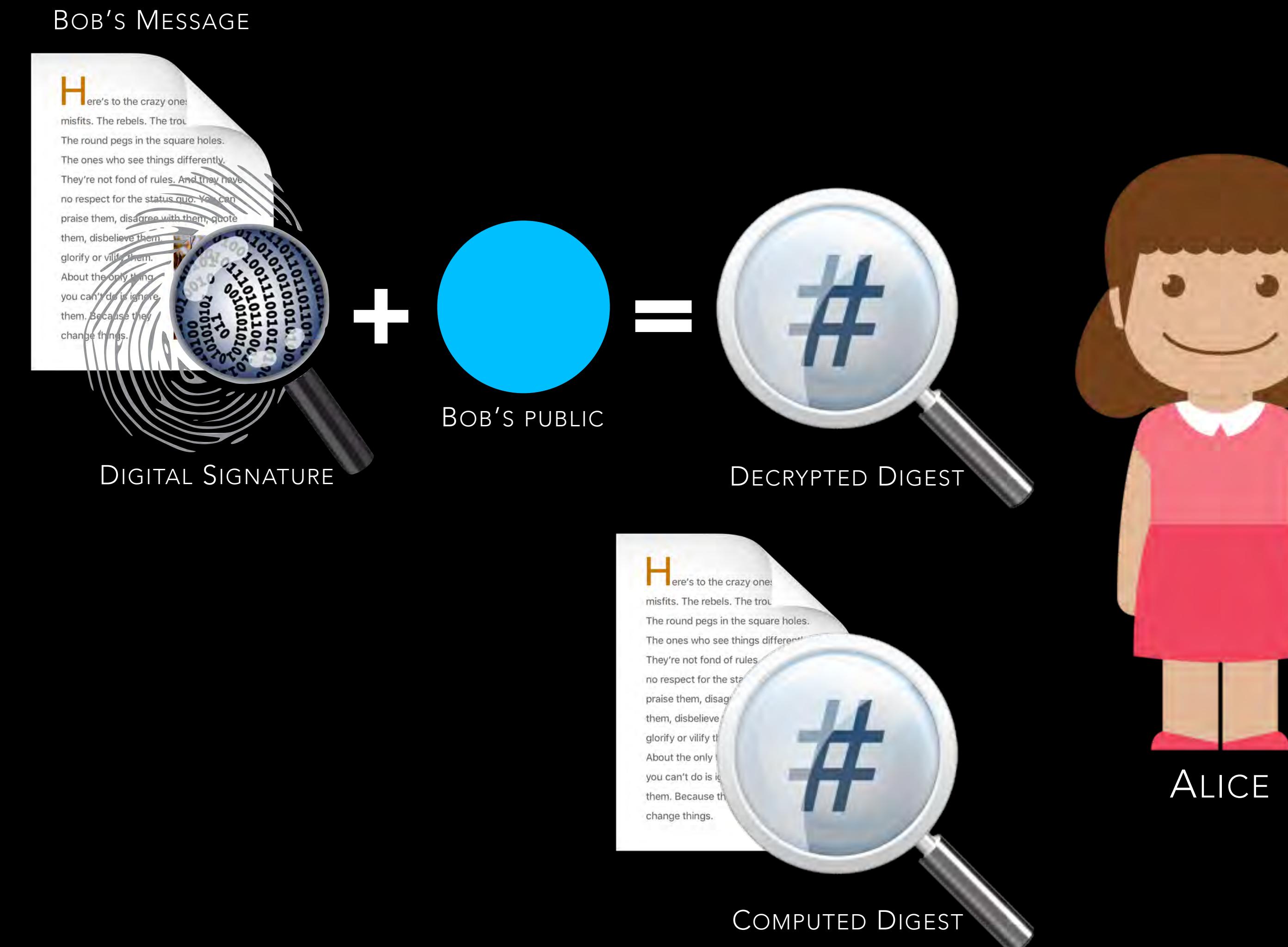


3. Alice decrypts the digital signature with the Bob's public key to produce the decrypted digest.



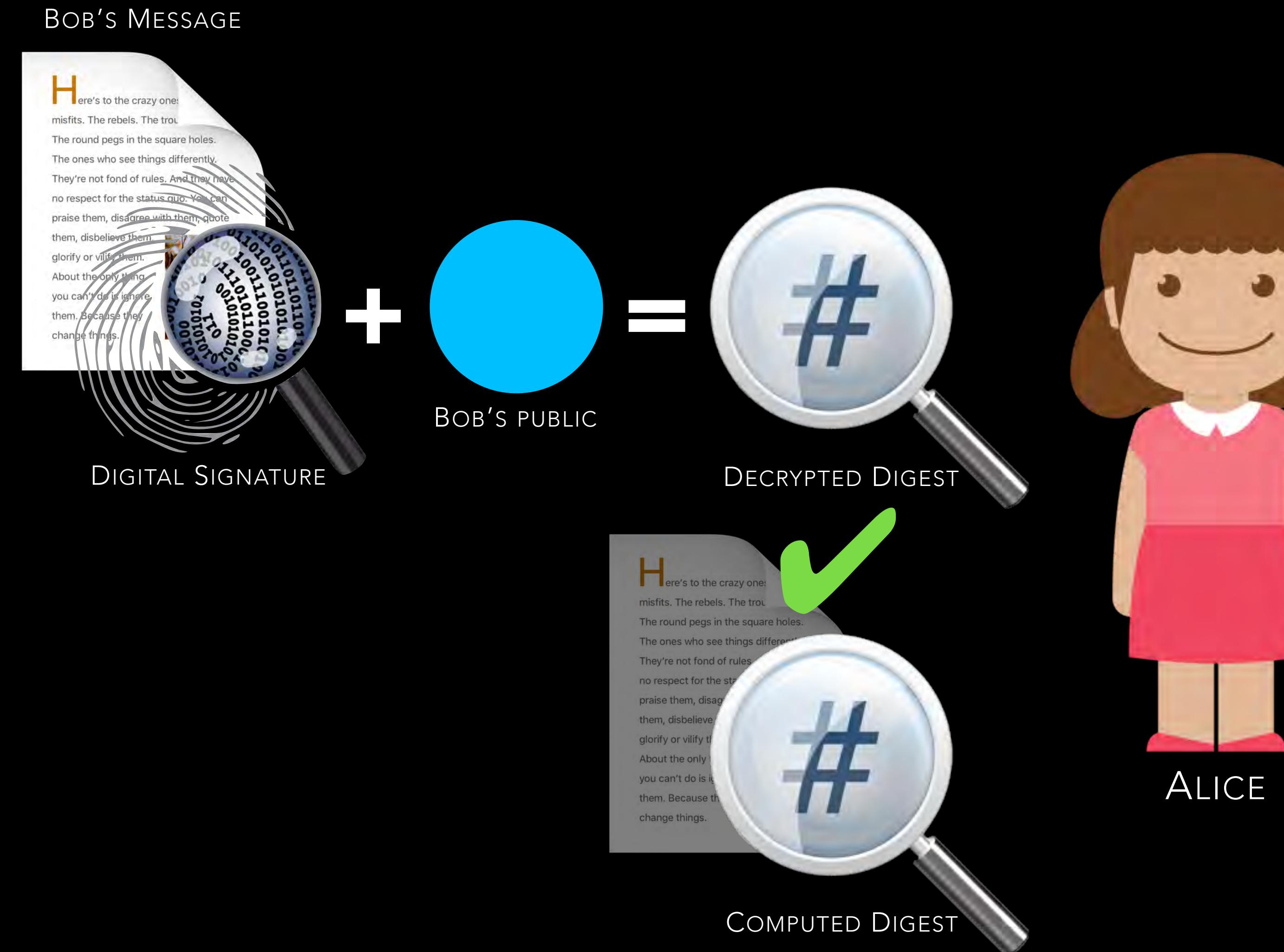
# PUBLIC KEY CRYPTOGRAPHY – SIGNATURES

3. Alice decrypts the digital signature with the Bob's public key to produce the decrypted digest.
4. Alice computes the message hash to produce the computed digest.



# PUBLIC KEY CRYPTOGRAPHY – SIGNATURES

3. Alice decrypts the digital signature with the Bob's public key to produce the decrypted digest.
4. Alice computes the message hash to produce the computed digest.
5. If the decrypted digest and the computed digest match, the message must have been signed by Bob and has not been modified.



# CERTIFICATES



# WHAT IS A PUBLIC KEY CERTIFICATE?



In cryptography, a **public key certificate** is an electronic document used to prove ownership of a public key.

# CONTENTS OF A PUBLIC KEY CERTIFICATE?



**INFORMATION ABOUT THE CERTIFICATE HOLDER:** name, email address, company name, the owner's public key, etc.

**A DIGITAL SIGNATURE FROM A CERTIFICATION AUTHORITY:** to ensure that the certificate has not been altered and to indicate the identity of the issuer.

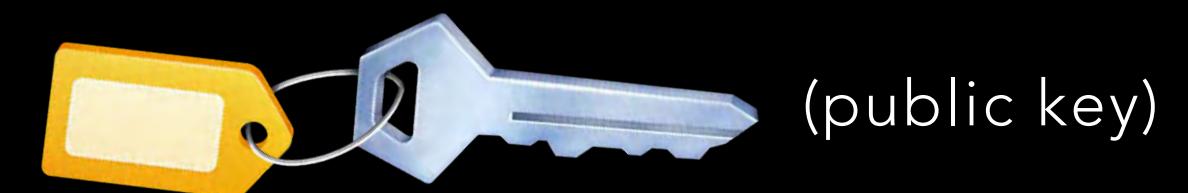
**VALIDITY PERIOD:** the certificate is not valid before or after this period.

**STRUCTURAL INFORMATION:** version, serial number, the message digest algorithm used to create the signature, and so on.

**CERTIFICATE EXTENSIONS** — attributes that contain additional information such as allowable uses for this certificate.

Item 1  
Item 2  
...

Extension 1  
Extension 2  
...



Tycho

d6225b8a5b3f1207a6cb56

Signing CA



iPhone

This is 7.

Mac      iPad

Apple Inc. www.apple.com

Safari is using an encrypted connection to [www.apple.com](https://www.apple.com).

Encryption with a digital certificate keeps information private as it's sent to or from the https website [www.apple.com](https://www.apple.com).

Symantec Corporation has identified [www.apple.com](https://www.apple.com) as being owned by Apple Inc. in Cupertino, California, US.

VeriSign Class 3 Public Primary Certification Authority - G5  
↳ Symantec Class 3 EV SSL CA - G3  
↳ www.apple.com

 **www.apple.com**  
Issued by: Symantec Class 3 EV SSL CA - G3  
Expires: Monday, 16 October 2017 at 01:59:59 Central European Summer Time  
✓ This certificate is valid



VeriSign Class 3 Public Primary Certification Authority - G5  
↳ Symantec Class 3 EV SSL CA - G3  
↳ www.apple.com



### www.apple.com

Issued by: Symantec Class 3 EV SSL CA - G3

Expires: Monday, 16 October 2017 at 01:59:59 Central European Summer Time

This certificate is valid

#### ► Trust

#### ▼ Details

Subject Name

Inc. Country

US

Inc. State/Province

California

Business Category

Private Organization

Serial Number

C0806592

Country

US

Postal Code

95014

State/Province

California

Locality

Cupertino

Street Address

1 Infinite Loop

Organization

Apple Inc.

Organizational Unit

Internet Services for Akamai

Common Name

www.apple.com

Issuer Name

Country

US

Organization

Symantec Corporation

Organizational Unit

Symantec Trust Network

Common Name

Symantec Class 3 EV SSL CA - G3



Hide Certificate

OK



Mac

iPad

**Safari is using an encrypted connection to www.apple.com.**

Encryption with a digital certificate keeps information private as it's sent to or from the https website www.apple.com.

Symantec Corporation has identified www.apple.com as being owned by Apple Inc. in Cupertino, California, US.

**Symantec Class 3 EV SSL CA - G3**

Intermediate certificate authority

Expires: Tuesday, 31 October 2023 at 00:59:59 Central European Standard Time

 This certificate is valid

## ► Trust

## ▼ Details

## Subject Name

Country US

Organization Symantec Corporation

Organizational Unit Symantec Trust Network

## Common Name Symantec Class 3 EV SSL CA - G3

## Issuer Name

Country US

Organization VeriSign, Inc.

Organizational Unit VeriSign Trust Network

Organizational Unit (c) 2006 VeriSign, Inc. - For authorized use only

## Common Name VeriSign Class 3 Public Primary Certification Authority - G5

Serial Number 7E E1 4A 6F 6F EF F2 D3 7F 3F AD 65 4D 3A DA B4

Version 3

Signature Algorithm SHA-256 with RSA Encryption ( 1.2.840.113549.1.1.11 )

Parameters none

Not Valid Before Thursday, 31 October 2013 at 01:00:00 Central European Standard Time



Hide Certificate

OK

Mac iPad

Apple Inc. www.apple.com

Safari is using an encrypted connection to [www.apple.com](https://www.apple.com).

Encryption with a digital certificate keeps information private as it's sent to or from the https website [www.apple.com](https://www.apple.com).

Symantec Corporation has identified [www.apple.com](https://www.apple.com) as being owned by Apple Inc. in Cupertino, California, US.

VeriSign Class 3 Public Primary Certification Authority - G5

↳ Symantec Class 3 EV SSL CA - G3  
↳ www.apple.com

 **VeriSign Class 3 Public Primary Certification Authority - G5**

Root certificate authority  
Expires: Thursday, 17 July 2036 at 01:59:59 Central European Summer Time  
This certificate is valid

▶ Trust

▼ Details

Subject Name  
Country US  
Organization VeriSign, Inc.  
Organizational Unit VeriSign Trust Network  
Organizational Unit (c) 2006 VeriSign, Inc. - For authorized use only  
Common Name VeriSign Class 3 Public Primary Certification Authority - G5

Issuer Name  
Country US  
Organization VeriSign, Inc.  
Organizational Unit VeriSign Trust Network  
Organizational Unit (c) 2006 VeriSign, Inc. - For authorized use only  
Common Name VeriSign Class 3 Public Primary Certification Authority - G5

Serial Number 18 DA D1 9E 26 7D E8 BB 4A 21 58 CD CC 6B 3B 4A  
Version 3

Signature Algorithm SHA-1 with RSA Encryption ( 1.2.840.113549.1.1.5 )  
Parameters none

Not Valid Before Wednesday, 8 November 2006 at 01:00:00 Central European Standard Time

?

Hide Certificate

OK

Support

Q

Bag

A large Apple logo is visible in the bottom right corner of the window.

Keychain Access

Click to unlock the System Roots keychain.

Search

**VeriSign Class 3 Public Primary Certification Authority - G5**

Root certificate authority  
Expires: Thursday, 17 July 2036 at 01:59:59 Central European Summer Time  
This certificate is valid

| Name  | Kind               | Date Modified | Expires                      | Keychain            |
|---|--------------------|---------------|------------------------------|---------------------|
| XRamp Global Certification Authority                                | certificate        | --            | 1 Jan 2035, 06:37:19         | System Roots        |
| WellsSecure Public Root Certificate Authority                       | certificate        | --            | 14 Dec 2022, 01:07:54        | System Roots        |
| VRK Gov. Root CA  | certificate        | --            | 18 Dec 2023, 14:51:08        | System Roots        |
| Visa Information Delivery Root CA                                   | certificate        | --            | 29 Jun 2025, 19:42:42        | System Roots        |
| Visa eCommerce Root   | certificate        | --            | 24 Jun 2022, 02:16:12        | System Roots        |
| VeriSign Universal Root Certification Authority                     | certificate        | --            | 2 Dec 2037, 00:59:59         | System Roots        |
| VeriSign Class 4 Public Primary Certification Authority - G3        | certificate        | --            | 17 Jul 2036, 01:59:59        | System Roots        |
| <b>VeriSign Class 3 Public Primary Certification Authority - G5</b> | <b>certificate</b> | <b>--</b>     | <b>17 Jul 2036, 01:59:59</b> | <b>System Roots</b> |
| VeriSign Class 3 Public Primary Certification Authority - G4        | certificate        | --            | 19 Jan 2038, 00:59:59        | System Roots        |
| VeriSign Class 3 Public Primary Certification Authority - G3        | certificate        | --            | 17 Jul 2036, 01:59:59        | System Roots        |
| VeriSign Class 2 Public Primary Certification Authority - G3        | certificate        | --            | 17 Jul 2036, 01:59:59        | System Roots        |
| VeriSign Class 1 Public Primary Certification Authority - G3        | certificate        | --            | 17 Jul 2036, 01:59:59        | System Roots        |
| UTN-USERFirst-Object  | certificate        | --            | 9 Jul 2019, 20:40:36         | System Roots        |
| UTN-USERFirst-Network Applications                                  | certificate        | --            | 9 Jul 2019, 20:57:49         | System Roots        |
| UTN-USERFirst-Hardware  | certificate        | --            | 9 Jul 2019, 20:19:22         | System Roots        |
| UTN-USERFirst-Client Authentication and Email                       | certificate        | --            | 9 Jul 2019, 19:36:58         | System Roots        |
| UTN - DATAcorp SGC  | certificate        | --            | 24 Jun 2019, 21:06:30        | System Roots        |
| UCA Root  | certificate        | --            | 31 Dec 2029, 01:00:00        | System Roots        |
| UCA Global Root   | certificate        | --            | 31 Dec 2037, 01:00:00        | System Roots        |
| TWCA Root Certification Authority                                   | certificate        | --            | 31 Dec 2030, 16:59:59        | System Roots        |
| TWCA Global Root CA   | certificate        | --            | 31 Dec 2030, 16:59:59        | System Roots        |
| TÜRKTRUST Elektronik Sertifika Hizmet Sağlayıcısı                   | certificate        | --            | 22 Dec 2017, 19:37:19        | System Roots        |
| TÜBİTAK UEKAE Kök Sertifika Hizmet Sağlayıcısı - Sürüm 3            | certificate        | --            | 21 Aug 2017, 13:37:07        | System Roots        |
| Trustis FPS Root CA   | certificate        | --            | 21 Jan 2024, 12:36:54        | System Roots        |
| Trusted Certificate Services  | certificate        | --            | 1 Jan 2029, 00:59:59         | System Roots        |
| TRUST2408 OCES Primary CA   | certificate        | --            | 3 Dec 2037, 14:11:34         | System Roots        |
| thawte Primary Root CA - G3   | certificate        | --            | 2 Dec 2037, 00:59:59         | System Roots        |

+ i Copy

176 items

# SO MANY KEYCHAINS

**LOGIN:** user specific items, typically login password

/Users/<username>/Library/Keychains/login.keychain

**ICLOUD/LOCAL ITEMS:** enabled/disabled cloud synced

/Users/<username>/Library/Keychains/<UUID>

**SYSTEM:** not user specific authentication assets

Only administrative users can make changes to it.

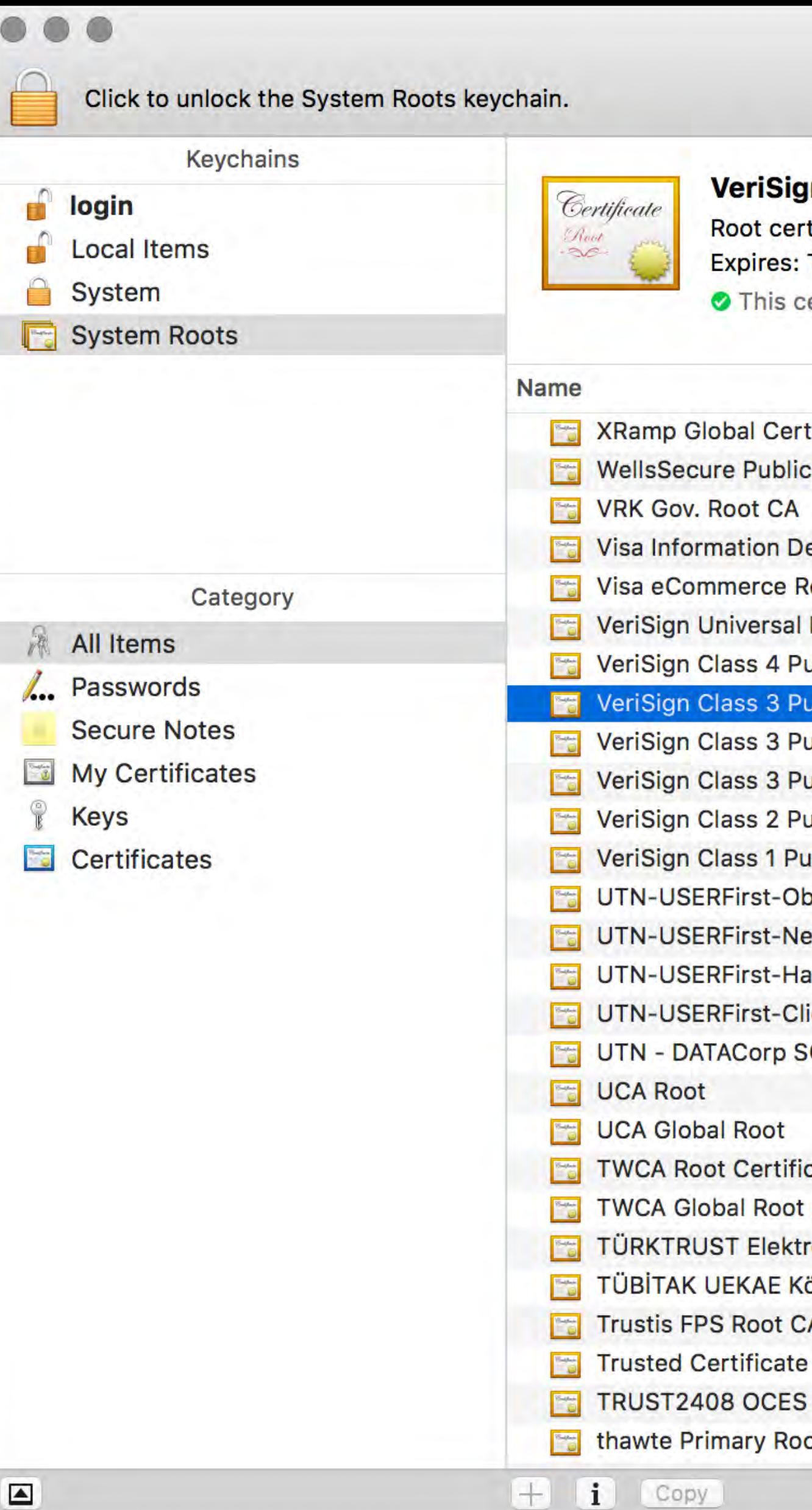
/Library/Keychains/System.keychain

**SYSTEM ROOTS:** system wide trusted root certificates.

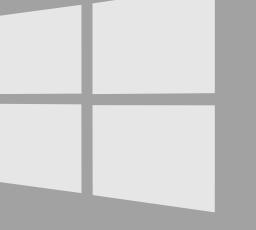
Only administrative users can change trust settings.

/System/Library/Keychains/SystemCACertificates.keychain

See also <https://support.apple.com/en-us/HT202858>



# ROOT CERTIFICATE STORES

|                        |   |   |  |   |
|------------------------|---|---|--|---|
| BROWSER                |   |   |  |   |
| OPERATING SYSTEM       | X    |    | ALL  |  |
| ROOT CERTIFICATE STORE |    |  Microsoft   | mozilla  |  |

The screenshot shows a web browser window with the following details:

- Address Bar:** Shows the URL [https://www.apple.com/certificateauthority/ca\\_program](https://www.apple.com/certificateauthority/ca_program).
- Toolbar:** Includes standard browser controls like back, forward, search, and refresh.
- Navigation Bar:** Features links for Mac, iPad, iPhone, Watch, TV, Music, Support, and a search icon.
- Content Area:** The main content is titled "Apple Root Certificate Program". Below it, a section titled "Program Requirements" contains the following text and list.

**Program Requirements**

To better protect Apple customers from security issues related to the use of public key infrastructure (PKI) certificates and enhance the experience for Apple users, Apple requires root certification authorities to meet certain criteria. Apple products, including our web browser Safari and Mail.app, use a common store for root certificates. Following are some highlights of the new criteria:

- Certification Authority (CA) providers are required to complete a Trust Principles and Criteria for Certification Authorities (WebTrust for Certification Authorities) audit or provide an equivalent third-party attestation. Additionally, CAs issuing SSL certificates must also complete a current Trust Services Principles and Criteria for Certification Authorities – SSL Baseline with Network Security audit. For more information about the WebTrust for Certification Authorities program sponsored by The American Institute for Certified Public Accountant's (AICPA) or to obtain a copy of the criteria, see <http://www.webtrust.org/>. If you have received an audit from a different program, the burden is on the CA to prove equivalency to WebTrust for CAs.
- A maximum of three roots per CA provider can be accepted because each additional root negatively impacts users by increasing download time.
- Apple requires a test certificate issued from each CA provider's root(s) for testing purposes. We recommend that you send Apple a URL of a publicly accessible server where certificates issued from your roots can be verified.
- All new root certification authorities for OS X are made seamlessly available to end users through the Software Update mechanism. This provides maximum flexibility for CA providers and Apple to respond immediately in the event of an unforeseen security issue.
- Your root certificate must provide broad business value to Apple platform customers. For example, root certificates that are used internally within an organization are not acceptable for the root program.
- For Extended Validation certificates issued from your root, issued certificates must support the Online Certificate Status Protocol (OCSP). The OCSP URL should point to a location that is publicly accessible.
- For non-Extended Validation certificates issued from your root, issued certificates must support either the OCSP or the CRL distribution point extension. The CRL distribution point should point to a location that is publicly accessible.
- Root certificates must conform to the standard set forth in RFC 3280.

[https://www.apple.com/certificateauthority/ca\\_program.html](https://www.apple.com/certificateauthority/ca_program.html)

# PUBLIC KEY INFRASTRUCTURE

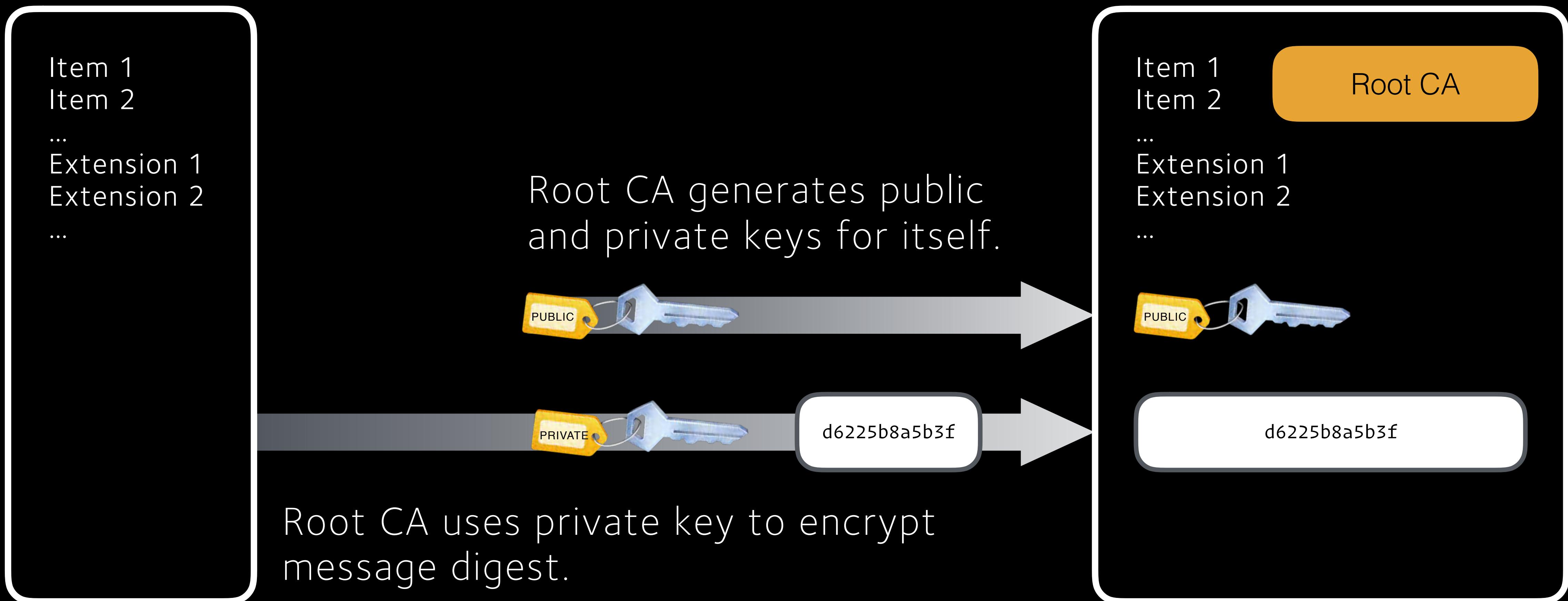


A public key infrastructure typically consists of:

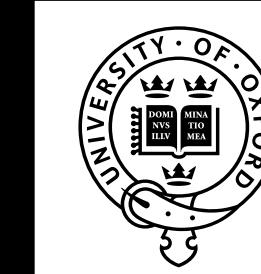
- A **CERTIFICATE AUTHORITY (CA)** that stores, issues and signs the digital certificates.
- A **REGISTRATION AUTHORITY (RA)** which verifies the identity of entities requesting their digital certificates to be signed by and stored at the CA.
- A (third-party) **VALIDATION AUTHORITY (VA)**.
- A **CENTRAL DIRECTORY**—i.e., a secure location in which to store and index keys.
- A **CERTIFICATE MANAGEMENT SYSTEM** managing things like the access to stored certificates or the delivery of the certificates to be issued.
- A **CERTIFICATE POLICY**.

# CREATING A Root CA

Root CA assigns certificate attributes for own CA.



# CREATING AN INTERMEDIATE CA



# UNIVERSITY OF OXFORD

Root CA assigns  
certificate attributes

- Item 1
- Item 2

# Extension 1

# Extension 2

•

Root CA uses private key to encrypt message digest.

A close-up photograph of a silver metal key and a yellow plastic key tag. The tag has a white rectangular label in the center with the word "PRIVATE" printed in black capital letters. A metal keyring connects the tag to the key.

A close-up photograph of a standard blue metal key. A green plastic keychain tag is attached to its keyring. The tag has a rectangular shape with rounded corners and a small hole at the top center. The word "PRIVATE" is printed in bold, black, uppercase letters across the center of the tag. The background is solid black, making the blue key and green tag stand out.

A large, metallic blue key is shown against a black background. A green plastic key tag is attached to the shank of the key. The tag has the word "PUBLIC" printed on it in a bold, black, sans-serif font. The lighting highlights the metallic texture of the key and the vibrant green of the tag.

421c76d77563

Root CA uses own certificate to sign intermediate certificate.

# Certificates

rtificate to  
tificate.

# Item 1

# Item 2

# Extension 1

# Extension 2

1

A large, metallic blue key is shown in the background, angled diagonally. In the foreground, a bright green plastic keychain tag hangs from the key's split ring. The tag has a rectangular shape with rounded corners and a small hole at the top center. The word "PUBLIC" is printed in bold, black, uppercase letters in the center of the tag.

421c76d77563

Root CA

*Steve Jobs*

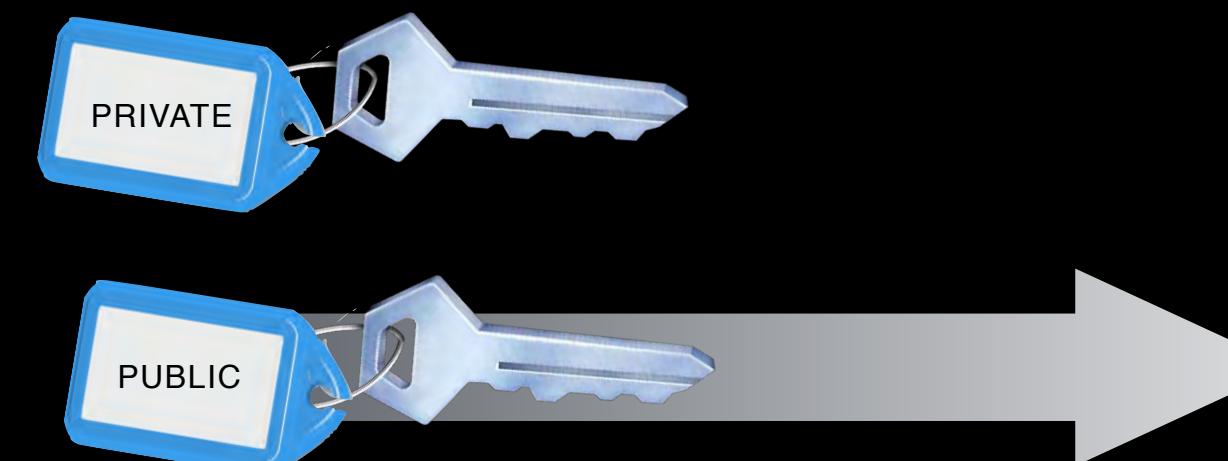
# CREATING AN USER CERTIFICATE



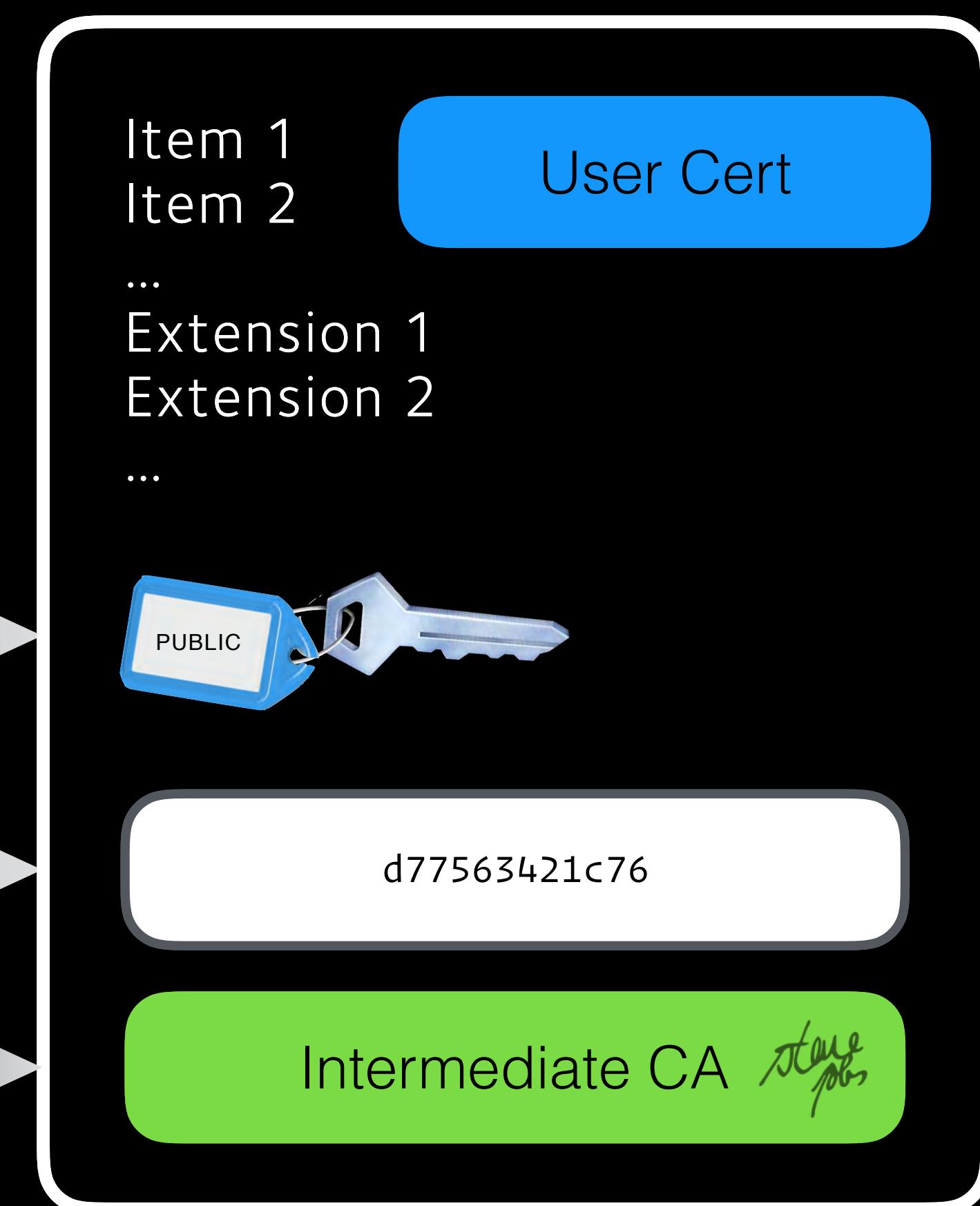
Intermediate CA assigns user certificate attributes



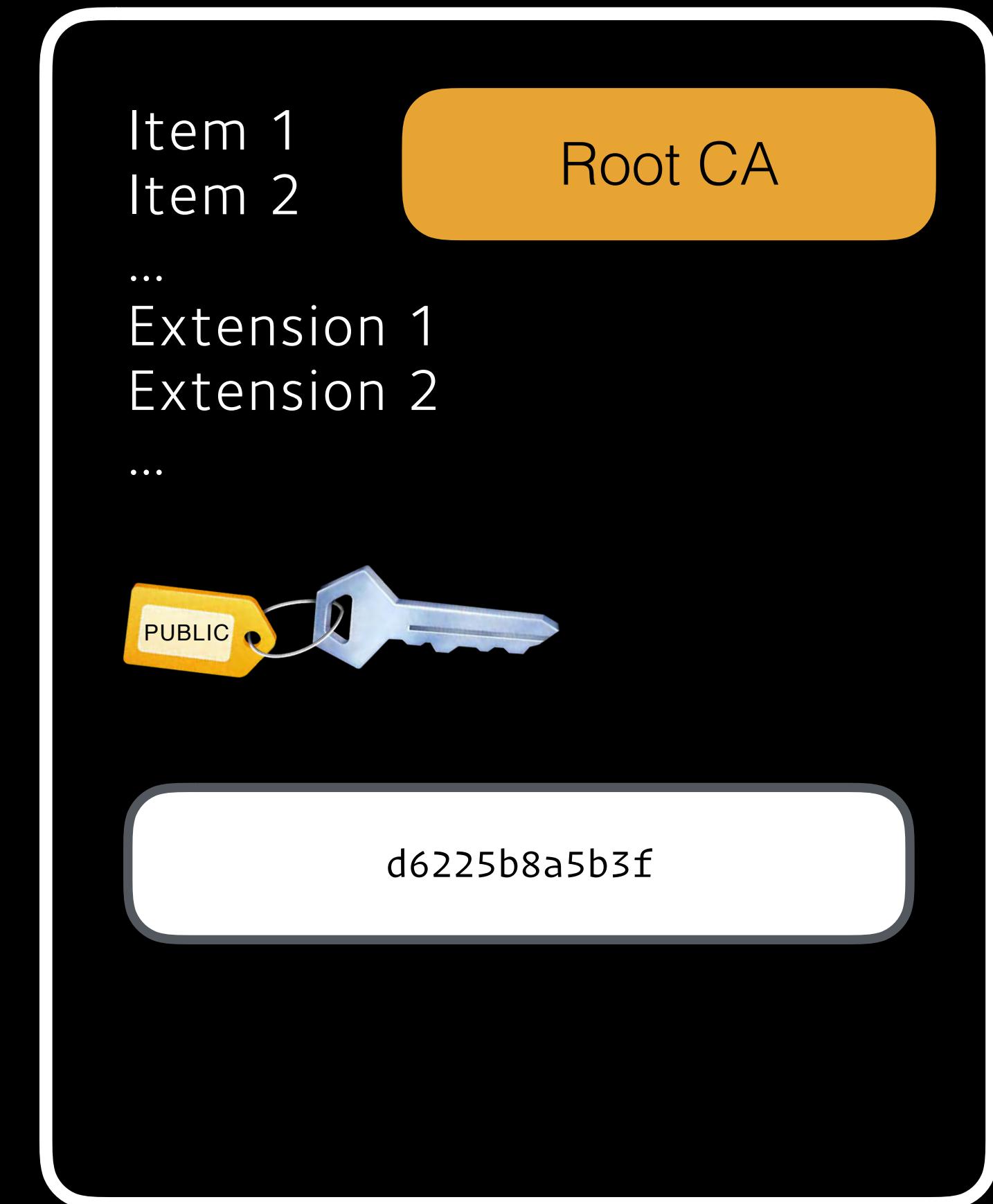
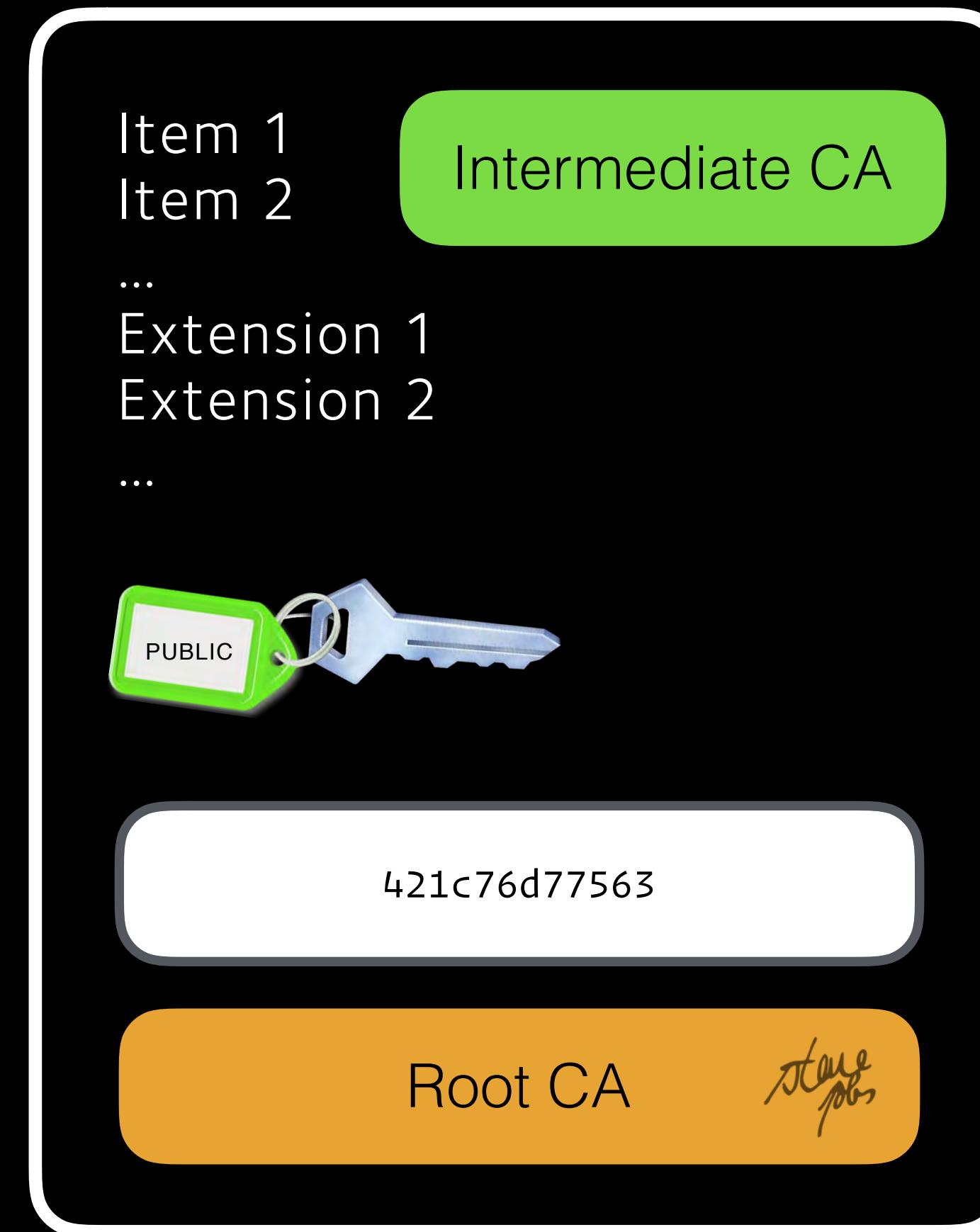
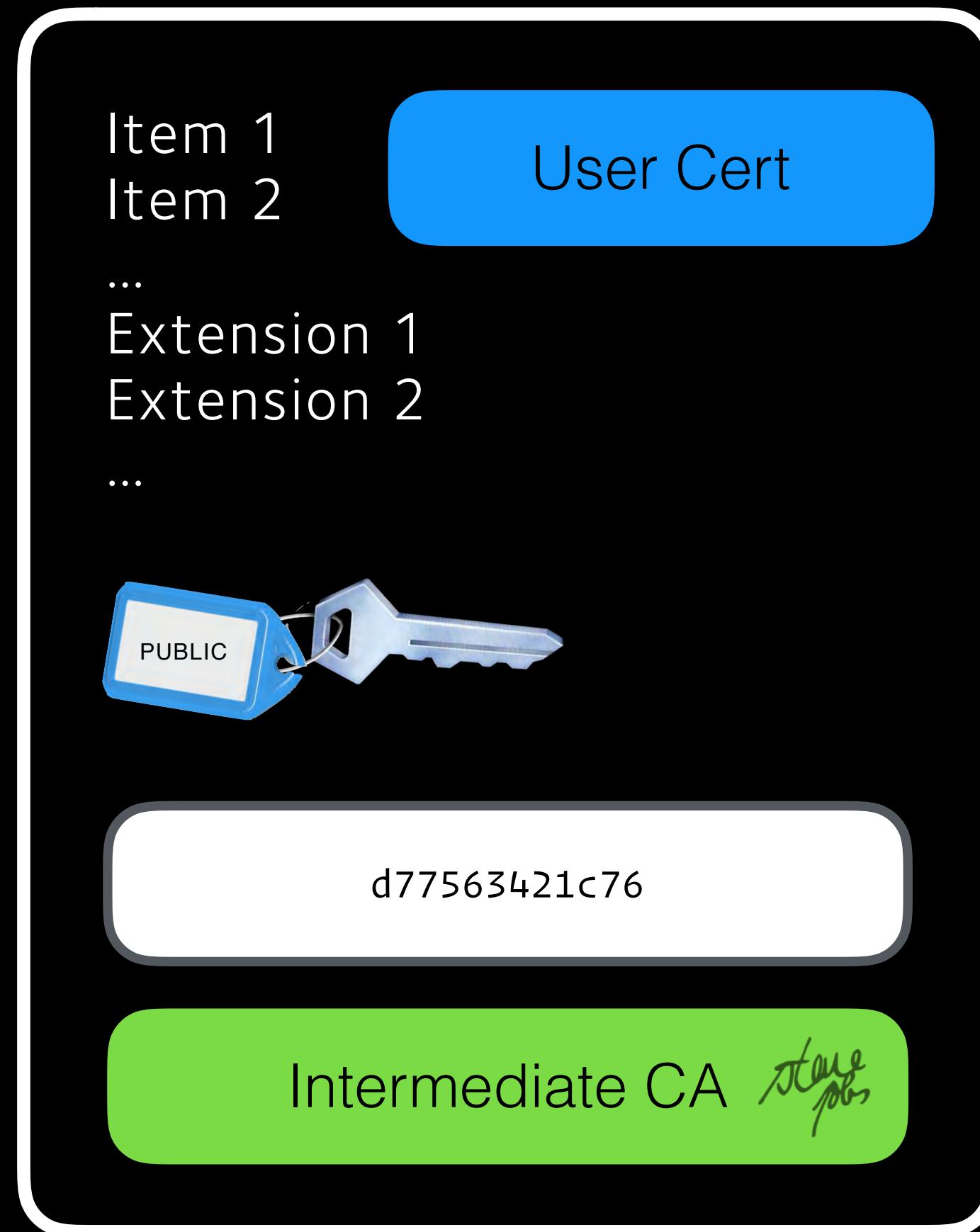
End user creates public and private key and provides its public key to the intermediate CA.



Intermediate CA uses own certificate to sign intermediate certificate.



# CERTIFICATE CHAIN



# CERTIFICATE REVOCATION LISTS



```
$ openssl crl -in apple-ca-root.crl -inform DER -text
```

Certificate Revocation List (CRL):

Version 2 (0x1)

Signature Algorithm: sha1WithRSAEncryption

Issuer: /C=US/O=Apple Inc./OU=Apple Certification Authority/CN=Apple Root CA

Last Update: Aug 17 02:42:03 2016 GMT

Next Update: Dec 30 02:42:03 2016 GMT

CRL extensions:

X509v3 Authority Key Identifier:

keyid:2B:D0:69:47:94:76:09:FE:F4:6B:8D:2E:40:A6:F7:47:4D:7F:08:5E

No Revoked Certificates.

Signature Algorithm: sha1WithRSAEncryption

af:67:57:57:bd:51:3f:b3:69:aa:02:[...]:c9:de:9c:c6

-----BEGIN X509 CRL-----

```
MIIB0DCBuQIBATANBgkqhkiG9w0BAQUFADBiMQswCQYDVQQGEwJVUzETMBEGA1UE  
ChMKQXBwbGUgSW5jLjEmMCQGA1UECxMdQXBwbGUgQ2VydGlmaWNhdGlvbiBBdXRo  
[...]/NdyVvod94PCz2cvNxlrhc3yowAAfpouLNne/QsDjfJ3pzG
```

-----END X509 CRL-----

# CERTIFICATE REVOCATION LISTS



```
$ openssl crl -in apple-wwdrca.crl -inform DER -text
```

Certificate Revocation List (CRL):

Version 2 (0x1)

Signature Algorithm: sha1WithRSAEncryption

Issuer: /C=US/O=Apple Inc./OU=Apple Worldwide Developer Relations/CN=Apple Worldwide Developer Relations Certification Authority

Last Update: Oct 5 02:21:44 2016 GMT

Next Update: Oct 19 02:21:44 2016 GMT

CRL extensions:

X509v3 Authority Key Identifier: keyid:88:27:17:09:A9:B6:18:60:[...]:47:59:C5:52:54:A3:B7

X509v3 CRL Number: 4576

X509v3 Issuing Distribution Point: critical

0B.@.>.<http://developer.apple.com/certificationauthority/wwdrca.crl

Revoked Certificates:

Serial Number: 08D53EDF8EE90515

Revocation Date: Mar 4 00:45:10 2016 GMT

CRL entry extensions:

X509v3 CRL Reason Code: Key Compromise

[...]

# CERTIFICATE REVOCATION LISTS



```
$ openssl crl -in apple-wwdrca.crl -inform DER -text | grep "Serial Number:" | wc -l
```

2.454.163

# CERTIFICATE REVOCATION LISTS



- A CRL is generated and published periodically, often at a defined interval.
- CRLs usually carry a digital signature associated with the CA by which they are published.
- Part of every good CA Policy
- Should be part of every signing certificate as certificate extension:  
CRL Distribution Points (2.5.29.31)
- Specified in RFC5280  
<https://tools.ietf.org/html/rfc5280>



# ONLINE CERTIFICATE STATUS PROTOCOL

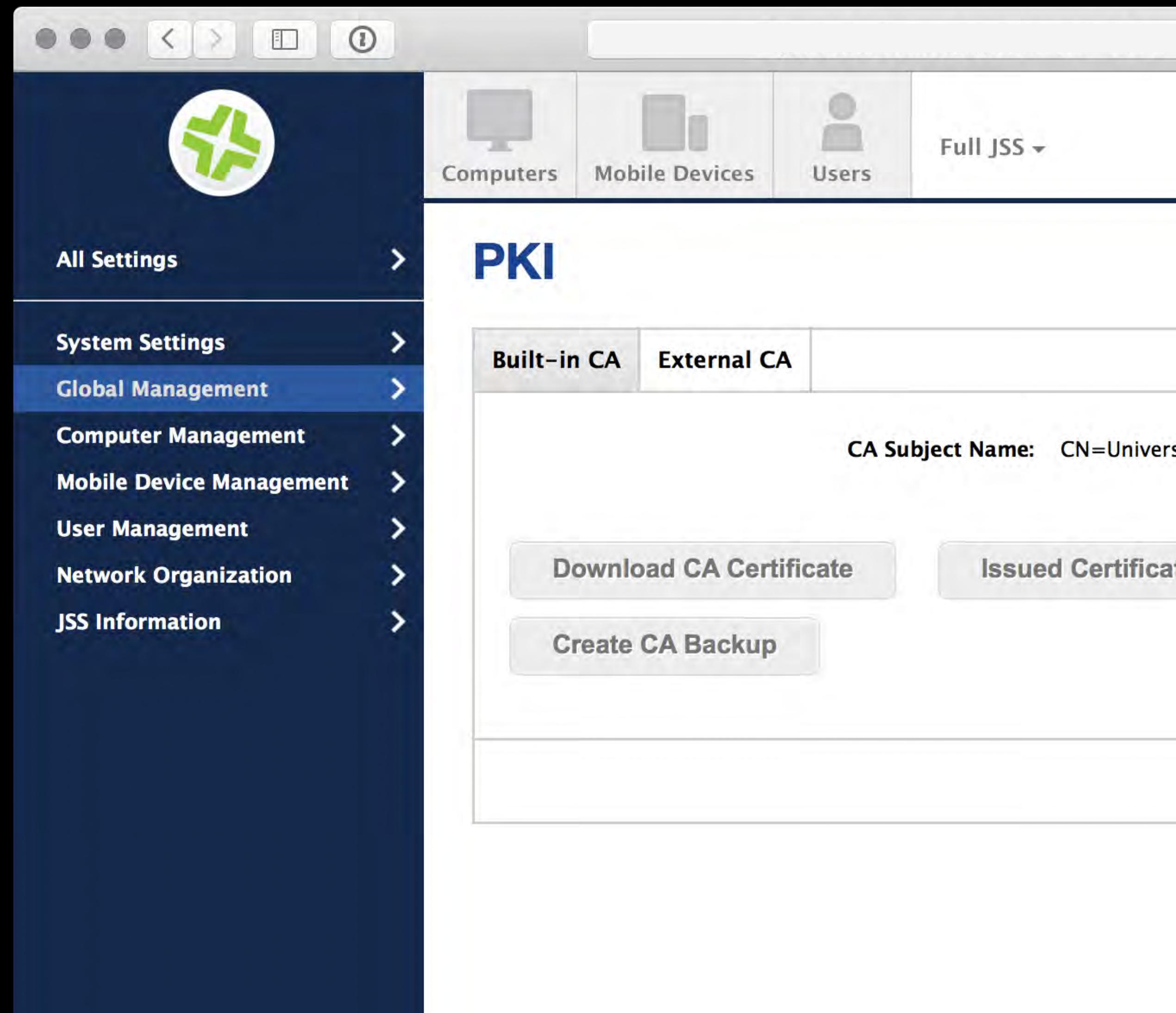


- Messages communicated via OCSP are encoded in ASN.1 over HTTP
- OCSP servers are often also called OCSP responders ("request/response" pattern)  
Signed responses signify that the certificate specified in the request is 'good', 'revoked', or 'unknown'.
- More efficient than CRLs (less bandwidth, client library code, and client resource)
- OCSP discloses to the responder that a particular network host used a particular certificate at a particular time.
- Specified in RFC6960

<https://tools.ietf.org/html/rfc6960>

# PKI IMPLEMENTATIONS

- Microsoft Certification Authority roles
- OpenSSL
- EJBCA 
- OpenCA PKI Research Labs 
- JAMF Software Server and other MDMs



letsencrypt.org

LINUX FOUNDATION COLLABORATIVE PROJECTS

Let's Encrypt

Documentation Get Help Donate ▾ About Us ▾

Let's Encrypt is a new Certificate Authority:  
**It's free, automated, and open.**

Get Started

FROM OUR BLOG

Oct 1, 2016

ISRG Legal Transparency Report, January 2016 - June 2016

The trust of our users is ISRG's most critical asset.

mozilla Akamai CISCO E

OVH chrome IdenTrust Internet Society

A screenshot of a web browser displaying the Let's Encrypt website at letsencrypt.org. The page features a large central banner with a geometric background of blue and yellow triangles. The text "Let's Encrypt is a new Certificate Authority: It's free, automated, and open." is displayed in a large, bold font. Below this is a blue rectangular button with the text "Get Started". At the top of the page, there is a navigation bar with links for Documentation, Get Help, Donate, and About Us. The URL "letsencrypt.org" is visible in the address bar, along with the text "LINUX FOUNDATION COLLABORATIVE PROJECTS". The overall design is clean and modern, with a focus on the central message about the new certificate authority.

Thawte, Inc. www.thawte.com/ssl/

Contact Us +1 888 484 2983 / +1 520 477 3128 Chat sales@thawte.com Login Change Country

Products Partners Support Resources My Account SEARCH



## Products

SSL for the Enterprise

SSL Certificates [Compare All]

- SSL Web Server Certificates with EV
- SSL Web Server Certificates
- SSL 123 Certificates
- SAN/UC Capable Certificates
- Wildcard SSL Certificates
- SSL123 Wildcard

Code Signing Certificates

Thawte Trusted Site Seal

US Home > Products > SSL Certificates

Email Share Print

# SSL Certificates

Find the best SSL Certificate for your business

|  | SSL Web Server with EV   | SSL Web Server   | SSL123   |
|--|--|--|--|
| Issuance Time                              | Most certificates issued in <b>1-3 days</b>  | Most certificates issued in <b>one day</b>   | Most certificates issued in <b>minutes</b>   |
| Price: 1 year                              | <b>\$299</b><br><input type="checkbox"/> add wildcard + \$300<br><b>BUY NOW</b> <b>RENEW</b> | <b>\$199</b><br><input type="checkbox"/> add wildcard + \$596<br><b>BUY NOW</b> <b>RENEW</b> | <b>\$149</b><br><input type="checkbox"/> add wildcard + \$596<br><b>BUY NOW</b> <b>RENEW</b> |
| Browser Display                            | Your business https://   | https://www...   | https://www...   |
| Identity validation and customer assurance | Prominent visible assurance to increase trust and boost customer confidence                  | Visible assurance to customers that your website and domain are tied to your organization.   | SSL encryption with padlock icon   |
| Warranty (USD)                             | \$1,500,000  | \$1,250,000  | \$500,000  |
| Validity Options                           | 1-2 years  | 1-3 years  | 1-3 years  |

## Contact Sales

US Toll-Free:

+1 888 484 2983

US Direct:

+1 520 477 3128

South Africa:

+353 1 793 9142

Germany:

+49 69 3807 89081

France:

+33 1 57 32 42 68

UK:

+44 203 450 5486

[Submit Inquiry Online](#)



## Live Help

Sales Chat

Support Chat



Norton



PRODUCTS

SERVICES

SOLUTIONS

SUPPORT CENTER

SECURITY CENTER

Website Security / SSL/TLS Certificates

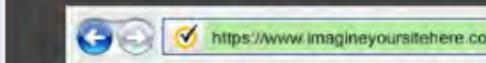
## Choose the Right SSL Certificates

Chat unavailable | Support | Account Login

### Choose the Right SSL Certificates

Helpful information to find the right SSL Certificates

### SSL Certificates with Visible SSL Protection



Guard against phishing with green address bar

### SSL Certificates with Strong encryption options

ECC, DSA and RSA Encryption options available

### Wildcard SSL Certificates

Protect multiple subdomains with one certificate

### Enterprise Solutions

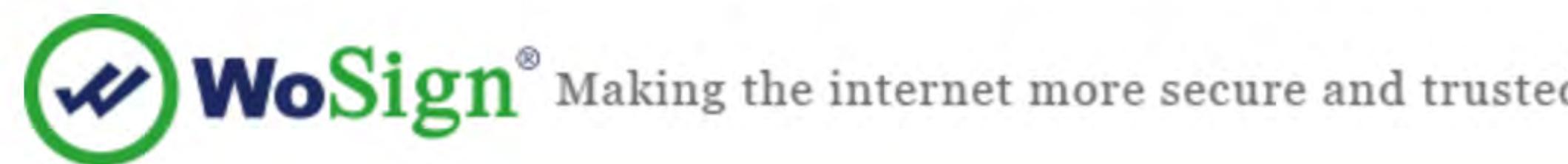
Complete Website Security

### Advantages of Symantec SSL Certificates

Symantec SSL/TLS certificates, formerly by VeriSign, uses industry-leading SSL encryption across all products, with various solutions for website and server security. Extended Validation (EV) SSL certificates will increase customers' confidence and help your website reach its full potential. Our 'Pro' SSL products offer ECC encryption, strong security on a short key length. Wildcard SSL certificate protects multiple subdomains under one SSL certificate. Compare and buy Symantec SSL Certificates here, to make sure your customers are safe from search to browse to buy.

### Compare SSL Certificates

| Visible SSL Protection    |                         |                         |                         |                         |                         |
|---------------------------|-------------------------|-------------------------|-------------------------|-------------------------|-------------------------|
| Symantec SSL Certificates | Secure Site with EV     | Secure Site Pro with EV | Secure Site             | Secure Site Pro         | Secure Site Wildcard    |
| Buy Now                   | <a href="#">BUY NOW</a> |
| Renew Now                 | <a href="#">RENEW</a>   |
| Price: 1 year             | \$995                   | \$1,499                 | \$399                   | \$995                   | \$1999                  |
| Green Address Bar         | ✓                       | ✓                       |                         |                         |                         |



(+1) 844-8-WOSIGN



CHINESE

Live Chat

Partner Programs

Digital Certificate Store

Home

Products ▾

Price

Support ▾

News

About Us ▾

Contact Us

My Account

Partner

# Securing the Global Internet

## Hi-Tech, Made in CHINA

*The world-class reliable PKI system, The world-class best service team*



# Lists of available trusted root certificates in macOS

The macOS Trust Store contains trusted root certificates that are preinstalled with macOS.

## Blocking Trust for WoSign CA Free SSL Certificate G2

Certificate Authority WoSign experienced multiple control failures in their certificate issuance processes for the WoSign CA Free SSL Certificate G2 intermediate CA. Although no WoSign root is in the list of Apple trusted roots, this intermediate CA used cross-signed certificate relationships with StartCom and Comodo to establish trust on Apple products.

In light of these findings, we are taking action to protect users in an upcoming security update. Apple products will no longer trust the WoSign CA Free SSL Certificate G2 intermediate CA.

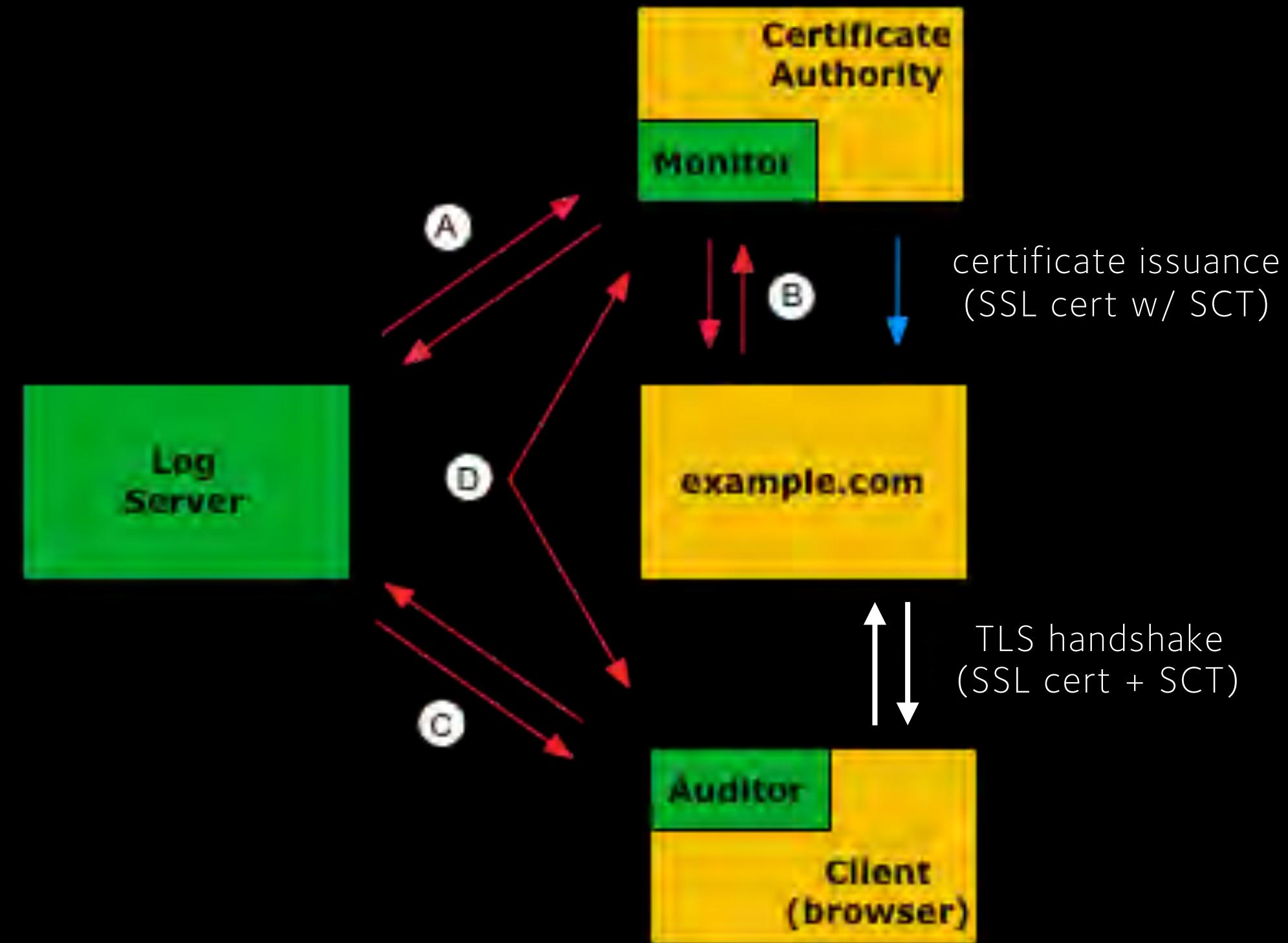
To avoid disruption to existing WoSign certificate holders and to allow their transition to trusted roots, Apple products will trust individual existing certificates issued from this intermediate CA and published to public [Certificate Transparency log servers by 2016-09-19](#). They will continue to be trusted until they expire, are revoked, or are untrusted at Apple's discretion.

As the investigation progresses, we will take further action on WoSign/StartCom trust anchors in Apple products as needed to protect users.

# CERTIFICATE TRANSPARENCY



- Open framework for monitoring and auditing of SSL certificates
  - detect SSL certificates that have been mistakenly issued by a CA or maliciously acquired from an otherwise unimpeachable CA
  - identify CAs that have gone rogue and are maliciously issuing certificates
- See <https://www.certificate-transparency.org>
- Specified in RFC6962  
<https://tools.ietf.org/html/rfc6962>



- Ⓐ Monitors watch logs for suspicious certs and verify that all logged certs are visible.
- Ⓑ Certificate owners query monitors to verify that nobody has logged illegitimate certs for their domain.
- Ⓒ Auditors verify that logs are behaving properly; they can also verify a particular cert has been logged.
- Ⓓ Monitors and auditors exchange information about logs to help detect forked or branched logs.

```
$ openssl x509 -in apple.pem -noout -text
```

Certificate:

Data:

Version: 3 (0x2)

Serial Number:

4c:d7:ab:ff:b5:b3:05:6d:d6:23:f3:0a:11:1b:95:f9

Signature Algorithm: sha256WithRSAEncryption

Issuer: C=US, O=Symantec Corporation, OU=Symantec Trust Network, CN=Symantec Class 3 EV SSL CA - G3

Validity

Not Before: Mar 28 00:00:00 2016 GMT

Not After : Oct 15 23:59:59 2017 GMT

Subject: 1.3.6.1.4.1.311.60.2.1.3=US/1.3.6.1.4.1.311.60.2.1.2=California/businessCategory=Private  
Organization/serialNumber=C0806592, C=US/postalCode=95014, ST=California, L=Cupertino/  
street=1 Infinite Loop, O=Apple Inc., OU=Internet Services for Akamai, CN=www.apple.com

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

RSA Public Key: (2048 bit)

Modulus (2048 bit):

00:e8:8d:83:fe:77:01:0d:8f:e5:28:51:60:c2:02:[...]:3f:2d

Exponent: 65537 (0x10001)

X509v3 extensions:

X509v3 Subject Alternative Name:

DNS:www.apple.com

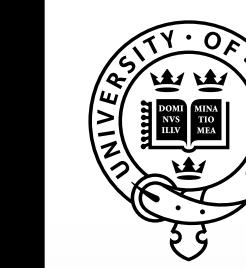
**X509v3 Key Usage: critical**

Digital Signature, Key Encipherment

**X509v3 Extended Key Usage:**

TLS Web Server Authentication, TLS Web Client Authentication

# EMAIL SIGNATURES – S/MIME



UNIVERSITY OF  
OXFORD

FW: [aa-dev] Accepting the "Apple Developer Program License Agreement" — Inbox

**Ben Goodstein**  
To: apple.developer-program-support@apple.com  
Reply-To: [aa-dev] [apple.developer-program-support@apple.com](#)  
[aa-dev] [apple.developer-program-support@apple.com](#)  
Security:  
  
On 04/10/2017, at 10:30 AM, Ben Goodstein wrote:  
I've agreed to the terms of the Apple Developer Program License Agreement.  
Ben  
--  
Ben Goodstein  
Senior Software Engineer  
IT Services, University of Oxford

AddTrust External CA Root  
↳ COMODO SHA-256 Client Authentication and Secure Email CA  
↳ ben.goodstein@it.ox.ac.uk

**ben.goodstein@it.ox.ac.uk**  
Issued by: COMODO SHA-256 Client Authentication and Secure Email CA  
Expires: Thursday, 25 May 2017 at 01:59:59 Central European Summer Time  
This certificate is valid

Details

OK

See More from Carmelo VELARDO

# EMAIL SIGNATURES – S/MIME



FW: [aa-dev] Accepting the "Apple Developer Program License Agreement" — Inbox

Ben Goodstein <ben.goodstein@it.ox.ac.uk>

To: apple-developer-program@lists.apple.com

Reply-To: [aa-dev] <apple-developer-program@lists.apple.com>

[aa-dev] I've agreed to the Apple Developer Program License Agreement

On 04/10/2013 10:45 AM, Ben Goodstein wrote:

I've agreed to the Apple Developer Program License Agreement

Ben  
--  
Ben Goodstein  
Senior Software Engineer  
IT Services

[See More from Ben Goodstein](#)

AddTrust External CA Root

↳ COMODO SHA-256 Client Authentication and Secure Email CA

↳ ben.goodstein@it.ox.ac.uk

1

A small circular portrait of a man with a beard and short hair, identified as Ben Goodstein.

**Public Key Info**

Algorithm RSA Encryption ( 1.2.840.113549.1.1.1 )

Parameters none

Public Key 256 bytes : 97 20 FB 98 79 38 66 86 ...

Exponent 65537

Key Size 2048 bits

Key Usage Verify, Wrap, Derive

Signature 256 bytes : 42 CA 95 4C 5A 3B AB F8 ...

**Extension** Key Usage ( 2.5.29.15 )

**Critical** YES

**Usage** Digital Signature, Key Encipherment

**Extension** Basic Constraints ( 2.5.29.19 )

From: Ben Goodstein  
To: Apple App Developers <apple-app-developers@maillist.ox.ac.uk>  
Subject: [aa-dev] FW: Accepting the "Apple Developer Program License Agreement"  
Date: Tue, 4 Oct 2016 13:31:21 +0000 [...]  
MIME-Version: 1.0

--B\_3558439839\_905099814

Content-type: text/plain;  
charset="UTF-8"  
Content-transfer-encoding: 7bit

On 04/10/2016, 15:29, "Ben Goodstein" <ben.goodstein@it.ox.ac.uk> wrote:  
> I've agreed to the updated terms, Marko will probably need to do the app  
> transfer, we're both away at a conference so I'll bug him about it later.  
>  
> Ben  
[...]

--B\_3558439839\_905099814

**Content-Type: application/pkcs7-signature; name="smime.p7s"**  
**Content-Transfer-Encoding: base64**  
**Content-Disposition: attachment; filename="smime.p7s"**

MIIQvwYJKoZIhvCNQcCoIIQsDCCEKwCAQExDzANBglghkgBZQMEAgEFADALBgkqhkiG9w0B  
BwGggg47MIIFsjCCBDKgAwIBAgIRAI7AiGB6QKPklqcDspN3tDcwDQYJKoZIhvCNQELBQA  
[...] xLmGVKR02enhIZz81iiHa6xZ0+0sJPp/Hg==

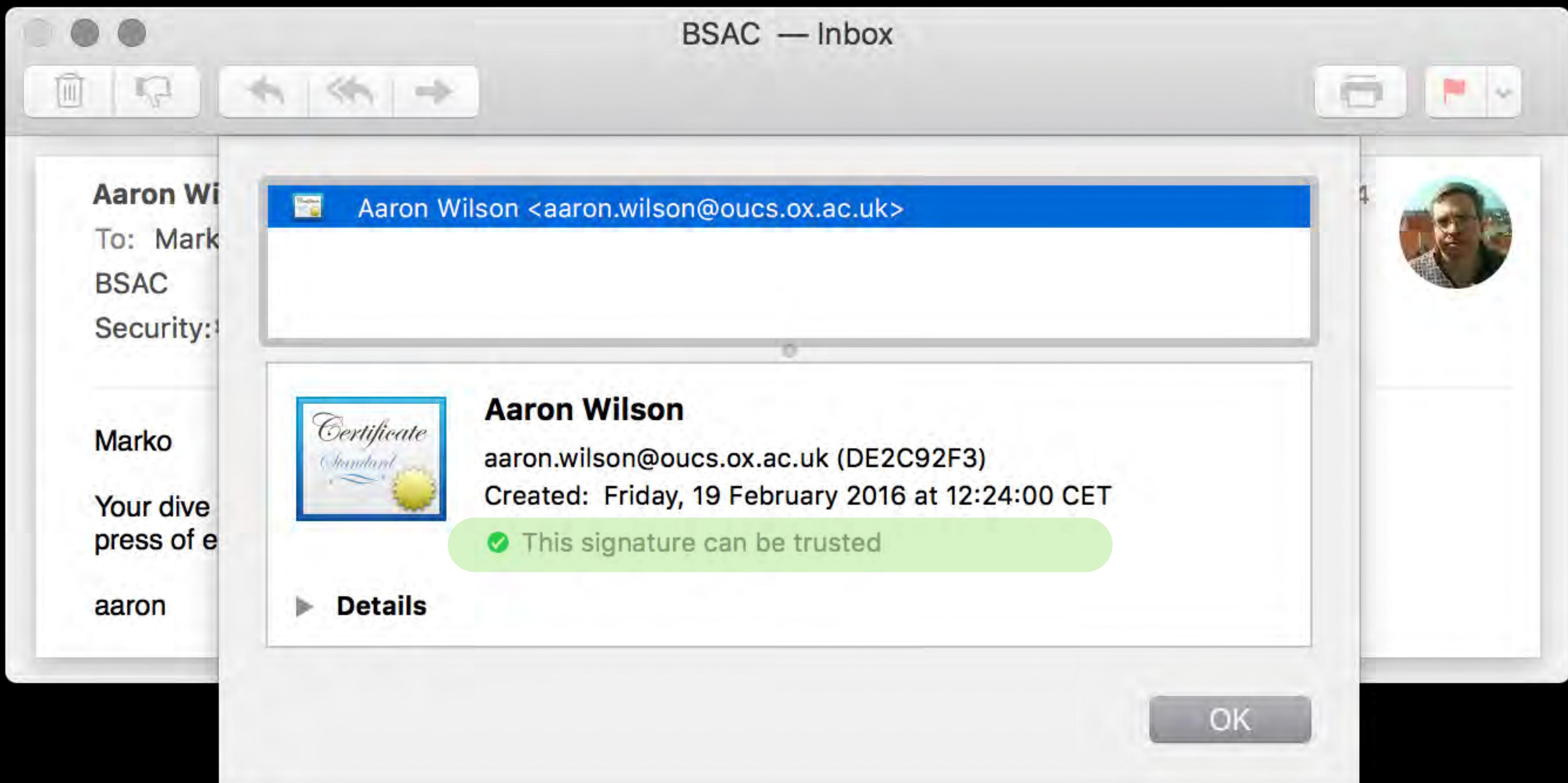
--B\_3558439839\_905099814--



# EMAIL SIGNATURES – OPENPGP



UNIVERSITY OF  
OXFORD



# EMAIL SIGNATURES – OPENPGP



UNIVERSITY OF  
OXFORD

BSAC — Inbox

Aaron Wilson <aaron.wilson@oucs.ox.ac.uk>

To: Marko

BSAC

Security: 4

Marko

Your dive press of e

aaron

**Signature**

Created: Friday, 19 February 2016 at 12:24:00 CET

Expires: No expiration is set on this signature

**Key**

Name: Aaron Wilson

E-Mail: aaron.wilson@oucs.ox.ac.uk

**Comment:**

Key ID: 798CA2C1DE2C92F3

Created: Friday, 30 July 2004 at 18:18:53 CEST

Expires: No expiration is set on this key

Algorithm: DSA

Ownertrust: 5



From: Aaron Wilson  
To: Marko Jung <marko.jung@it.ox.ac.uk>  
Date: Fri, 19 Feb 2016 11:24:00 +0000  
Subject: BSAC [...]  
MIME-Version: 1.0



--OROCMA9jn6tkzFBc  
Content-Type: text/plain; charset=us-ascii  
Content-Disposition: inline

Marko

Your dive packs have arrived; would you like them delivered to Ricky  
press of elsewhere ?

aaron

--OROCMA9jn6tkzFBc  
**Content-Type: application/pgp-signature; name="signature.asc"**  
**Content-Description: Digital signature**

-----BEGIN PGP SIGNATURE-----

Version: GnuPG v1

iEYEAARECAAYFA1bG+1AACgkQeYyiwd4skvNYKQCggwuxTgwalBG/7r/IkxxUnH1j  
hBkAn0GSi/9IjD3QgJ0twDUQZcx+gyF7  
=HQFH

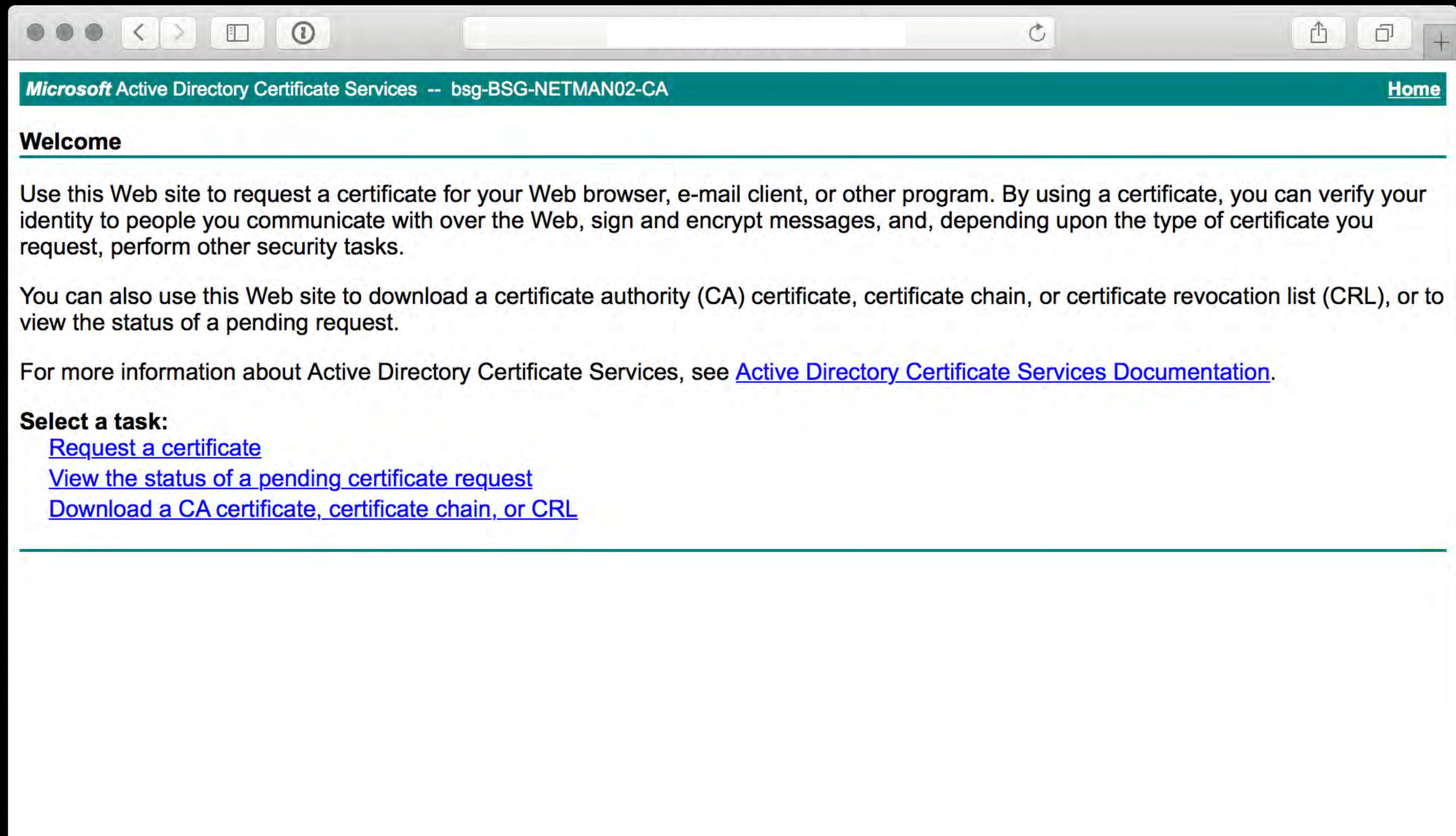
-----END PGP SIGNATURE-----

--OROCMA9jn6tkzFBc--



<https://gpgtools.org/>

# EXAMPLE: OBTAINING A CERTIFICATE

A screenshot of a web browser window showing the Microsoft Active Directory Certificate Services interface. The title bar reads "Microsoft Active Directory Certificate Services -- bsg-BSG-NETMAN02-CA". The main content area has a green header "Welcome". Below it, text explains the purpose of the site: "Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks." It also states: "You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request." At the bottom, under "Select a task:", there are three links: "Request a certificate", "View the status of a pending certificate request", and "Download a CA certificate, certificate chain, or CRL".

**Welcome**

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Active Directory Certificate Services, see [Active Directory Certificate Services Documentation](#).

**Select a task:**

[Request a certificate](#)

[View the status of a pending certificate request](#)

[Download a CA certificate, certificate chain, or CRL](#)

# EXAMPLE: OBTAINING A CERTIFICATE

A screenshot of a web browser window titled "Microsoft Active Directory Certificate Services -- bsg-BSG-NETMAN02-CA". The main content area is titled "Request a Certificate" and contains the following text:

Select the certificate type:

[User Certificate](#)  
[Blavatnik School of Government Certificate \(BSG\\_User\)](#)

Or, submit an [advanced certificate request](#).

# EXAMPLE: OBTAINING A CERTIFICATE



Microsoft Active Directory Certificate Services -- bsg-BSG-NETMAN02-CA [Home](#)

**Blavatnik School of Government Certificate (BSG\_User) - Identifying Information**

No further identifying information is required.

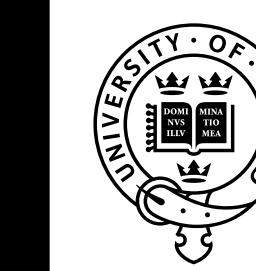
Please select a key strength:

Key Strength:

# EXAMPLE: OBTAINING A CERTIFICATE



A screenshot of a web browser window titled "Microsoft Active Directory Certificate Services -- bsg-BSG-NETMAN02-CA". The main content area displays the message "Certificate Issued" with a green underline. Below it, the text "The certificate you requested was issued to you." is shown. There are two buttons at the bottom: "Install this certificate" with a green icon and "Save response" with a checkbox.



Marko Jung

**Marko Jung**  
Issued by: bsg-BSG-NETMAN02-CA  
Expires: Tuesday, 5 October 2021 at 07:43:43 Central European Summer Time  
 This certificate is valid

**Trust**

**Details**

Subject Name

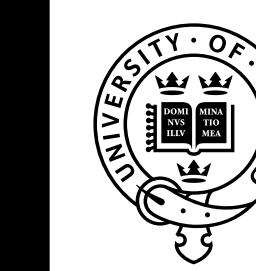
Common Name **Marko Jung**

Issuer Name

Public Key Info

Algorithm RSA Encryption ( 1.2.840.113549.1.1.1 )  
Parameters none  
Public Key 256 bytes : BB 38 4C 8E 22 E2 D9 C0 ...  
Exponent 65537  
Key Size 2048 bits  
Key Usage Encrypt, Verify, Wrap, Derive  
Signature 256 bytes : 94 F0 3C E0 A2 E7 2C EC ...

Extension Key Usage ( 2.5.29.15 )  
Critical YES  
Usage Digital Signature, Key Encipherment



Marko Jung

**Marko Jung**  
Issued by: bsg-BSG-NETMAN02-CA  
Expires: Tuesday, 5 October 2021 at 07:43:43 Central European Summer Time  
 This certificate is valid

**Trust**

**Details**

Subject Name

Common Name **Marko Jung**

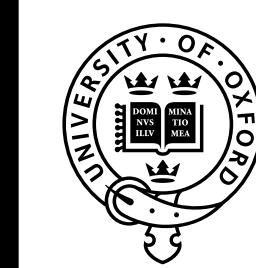
Issuer Name

Public Key Info

Algorithm RSA Encryption ( 1.2.840.113549.1.1.1 )  
Parameters none  
Public Key 256 bytes : BB 38 4C 8E 22 E2 D9 C0 ...  
Exponent 65537  
Key Size 2048 bits  
Key Usage Encrypt, Verify, Wrap, Derive  
Signature 256 bytes : 94 F0 3C E0 A2 E7 2C EC ...

Extension Key Usage ( 2.5.29.15 )  
Critical YES  
Usage Digital Signature, Key Encipherment

# CLIENT AUTHENTICATION



UNIVERSITY OF  
OXFORD



The Wi-Fi network "homerun1x" requires WPA2 enterprise credentials.

Mode: Automatic

Username:

Password:

Show password

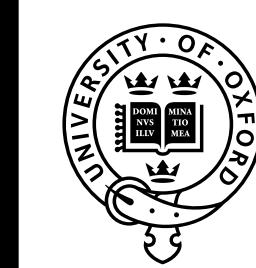
Remember this network

?

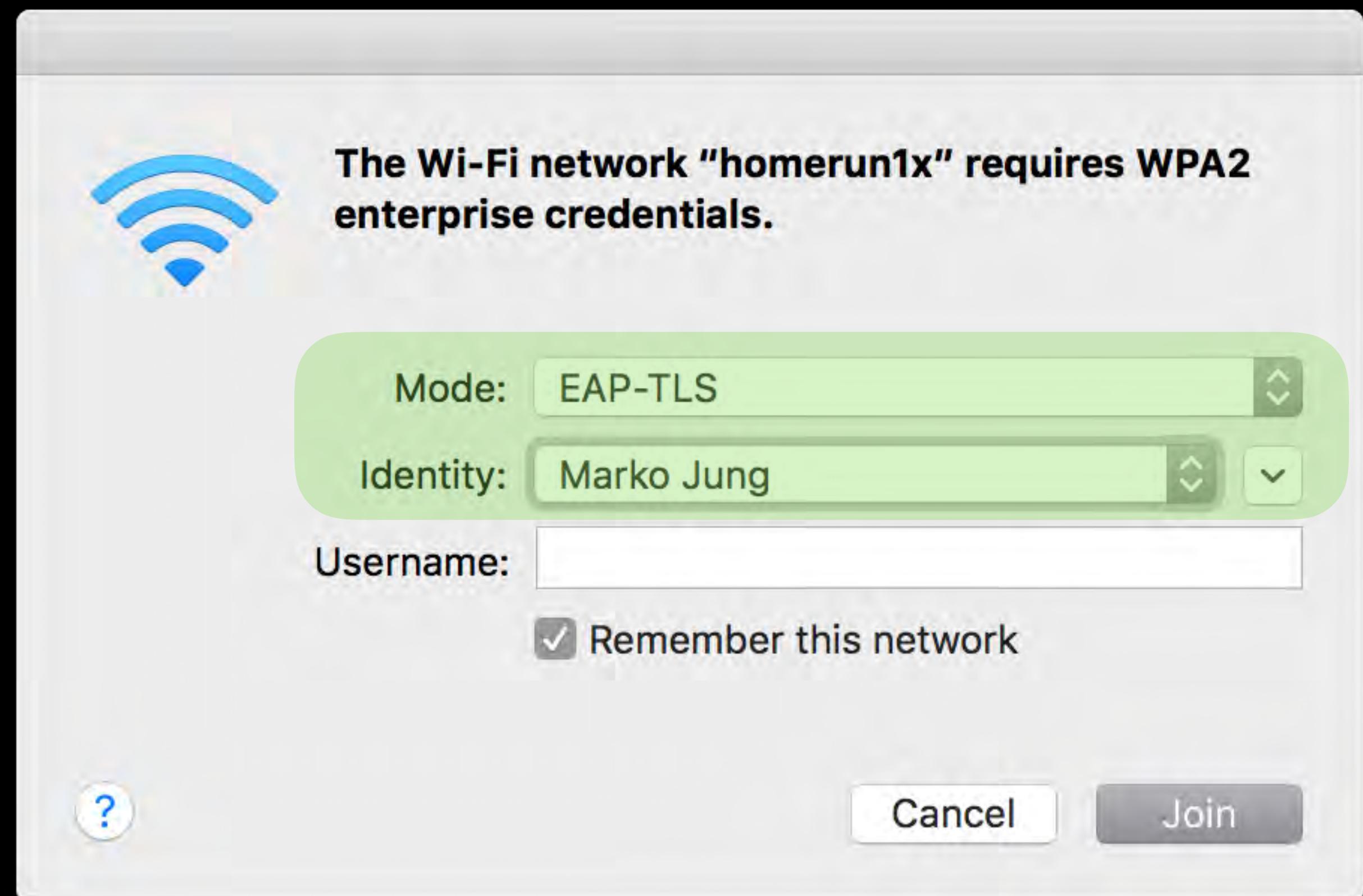
Cancel

Join

# CLIENT AUTHENTICATION



UNIVERSITY OF  
OXFORD



LIKELIHOOD YOU WILL GET CODE WORKING  
BASED ON HOW YOU'RE SUPPOSED TO INSTALL IT:

VERY LIKELY

APP STORE  
OR PACKAGE  
MANAGER

GITHUB LINK

SOURCEFORGE LINK

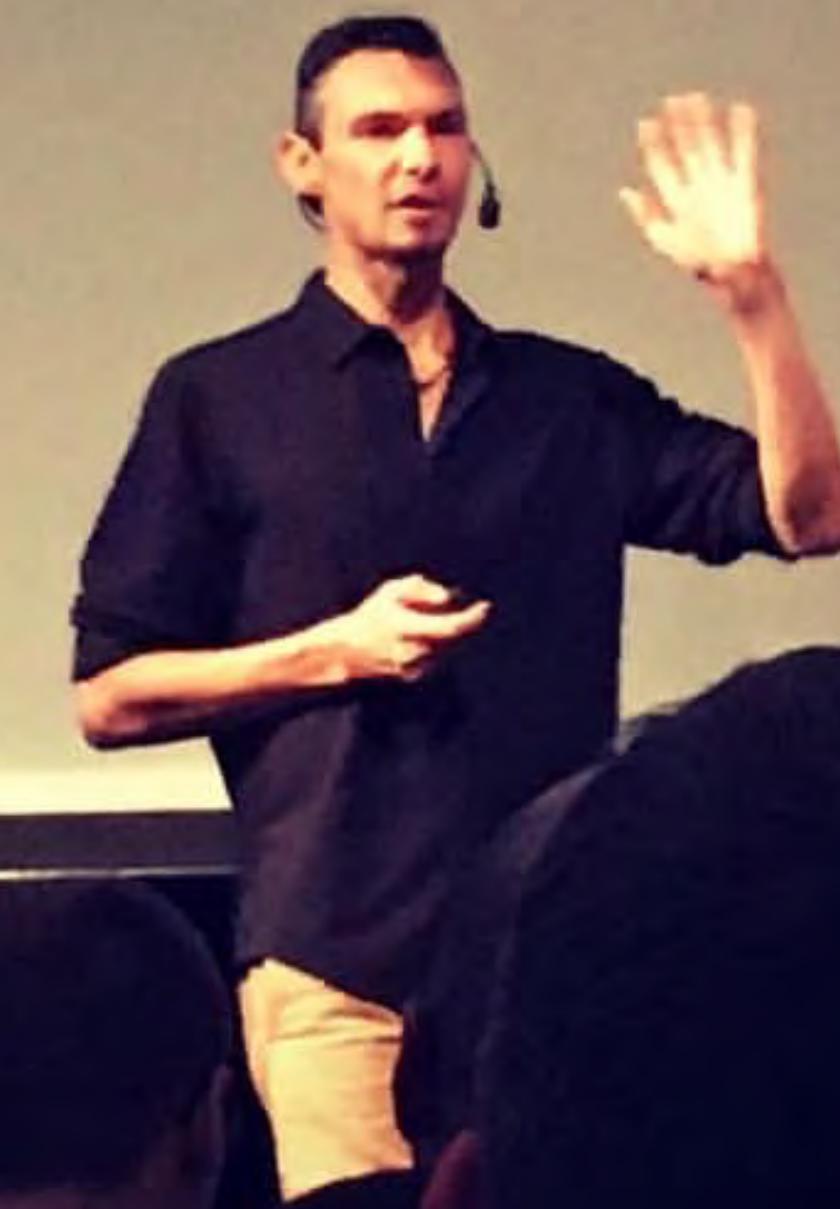
GEOCITIES/TRIPOD LINK

COPY-AND-PASTE  
EXAMPLE CODE FROM  
PAPER'S APPENDIX

ANYTHING THAT "REQUIRES  
ONLY MINIMAL CONFIGURATION  
AND TWEAKING"

UNLIKELY

**NOT AN EXPERT?  
PAY ONE!**



JSS BSG SCEP Testing\*\*

https://jss.orchard.ox.ac.uk/OSXConfigurationProfiles.html?id=50&o=r

Computers Mobile Devices Users Full JSS oucs0089

## BSG 802.1x EAP-TLS with CA chain and SCEP

Options Scope Show in JSS Dashboard

|   |  |
|---|--|
| <b>General</b>                              | <b>Network</b><br>1 Payload Configured |
| <b>Certificate</b><br>2 Payloads Configured |  |
| <b>SCEP</b><br>1 Payload Configured         |  |

**Network**

**Network Interface**  
Type of network interface on the device  
Wi-Fi

**Service Set Identifier (SSID)**  
Identification of the wireless network to connect to  
BSG

**Hidden Network**  
Enable if target network is not open or broadcasting

**Auto Join**  
Automatically join this wireless network

**Proxy Setup**  
Configures proxy settings to be used with this network  
None

**Security Type**  
Wireless network encryption to use when connecting  
WPA2 Enterprise

**Use as a Login Window configuration**  
User logs in to authenticate the Mac to the network

**Network Security Settings**  
Configurations options for 802.1X network authentication

Done History Logs Download Clone Delete Edit

Search Inventory Search VPP Content Licensed Software Policies Configuration Profiles Managed Preferences Restricted Software PreStage Imaging Mac App Store Apps Patch Reporting eBooks Smart Computer Groups Static Computer Groups Enrollment Invitations PreStage Enrollments Management Settings

JAMF software © 2002-2016 JAMF Software, LLC.

JSS BSG SCEP Testing\*\*

https://jss.orchard.ox.ac.uk/OSXConfigurationProfiles.html?id=50&o=r

Computers Mobile Devices Users Full JSS oucs0089

## BSG 802.1x EAP-TLS with CA chain and SCEP

Options Scope Show in JSS Dashboard

General User logs in to authenticate the Mac to the network

Network 1 Payload Configured Network Security Settings Configurations options for 802.1X network authentication

Certificate 2 Payloads Configured

SCEP 1 Payload Configured

Protocols Trust

Accepted EAP Types Authentication protocols supported on target network

TLS

TTLS

LEAP

PEAP

EAP-FAST

EAP-SIM

EAP-AKA

Username Username for connection to the network

Identity Certificate

Done History Logs Download Clone Delete Edit

Search Inventory >

Search VPP Content >

Licensed Software >

Policies >

Configuration Profiles > **Network**

Managed Preferences >

Restricted Software >

PreStage Imaging >

Mac App Store Apps >

Patch Reporting >

eBooks >

Smart Computer Groups >

Static Computer Groups >

Enrollment Invitations >

PreStage Enrollments >

Management Settings >

JAMF software © 2002-2016 JAMF Software, LLC.

JSS BSG SCEP Testing\*\*

https://jss.orchard.ox.ac.uk/OSXConfigurationProfiles.html?id=50&o=r

Computers Mobile Devices Users Full JSS oucs0089

Search Inventory >  
Search VPP Content >  
Licensed Software >  
  
Policies >  
Configuration Profiles > **BSG 802.1x EAP-TLS with CA chain and SCEP**  
Managed Preferences >  
Restricted Software >  
PreStage Imaging >  
Mac App Store Apps >  
Patch Reporting >  
eBooks >  
  
Smart Computer Groups >  
Static Computer Groups >  
  
Enrollment Invitations >  
PreStage Enrollments >  
  
Management Settings >

Options Scope Show in JSS Dashboard

General  
Network 1 Payload Configured  
**Certificate** 2 Payloads Configured  
SCEP 1 Payload Configured

**Certificate**

Certificate Name  
Name or description of the certificate credential  
BSG Root CA

Certificate

Subject: BSG-CA-CA  
Filename: cert-b.cer  
Issuer: CN=BSG-CA-CA  
Expires: 2030/10/07

Passphrase  
Passphrase used to secure the credentials

Verify Passphrase

**Certificate**

Certificate Name  
Name or description of the certificate credential

Done History Logs Download Clone Delete Edit

JAMF software © 2002-2016 JAMF Software, LLC.

JSS Edit OS X Configuration Profile x Marko

https://jss.orchard.ox.ac.uk/OSXConfigurationProfiles.html?id=51&o=u

Orchard Computers Mobile Devices Users Full JSS oucs0089

## BSG 802.1x EAP-TLS with CA chain and SCEP

Options Scope Self Service

|   |  |
|---|--|
| <b>General</b>                              | SCEP   |
| <b>Passcode</b><br>Not Configured           | <b>URL</b><br>The base URL for the SCEP server<br><code>https://pki.acme.org/certsrv/mscep/mscep</code>  |
| <b>Network</b><br>1 Payload Configured      | <b>Name</b><br>The name of the instance: CA-IDENT<br><code>BSG_USER</code>   |
| <b>VPN</b><br>Not Configured                | <input type="checkbox"/> <b>Display "Redistribute Profile" setting for this profile</b><br>Display a setting in the General payload that allows you to choose when you want to automatically redistribute this profile |
| <b>Certificate</b><br>2 Payloads Configured | <b>Subject</b><br>Representation of a X.500 name (e.g. "O=CompanyName, CN=Foo")<br><code>this requires</code>  |
| <b>SCEP</b><br>1 Payload Configured         | <b>Subject Alternative Name Type</b><br>The type of a subject alternative name<br><code>RFC 822 Name</code>  |
| <b>Directory</b><br>Not Configured          | <b>Subject Alternative Name Value</b><br>The value of a subject alternative name<br><code>minimal config</code>  |
| <b>Software Update</b><br>Not Configured    | <b>NT Principal Name</b><br>An NT principal name for use in the certificate request<br><code>and tweaking ;)</code>  |
| <b>Restrictions</b><br>Not Configured       |  |
| <b>Font</b><br>Not Configured               |  |
| <b>AirPlay</b>                              |  |

Cancel Save

# SIMPLE CERTIFICATE ENROLMENT PROTOCOL



- Aims to make the issuing of digital certificates as scalable as possible
- Simplistic request/response format over HTTP (preferably with TLS).  
Responses are returned as standard HTTP content, with a Content-Type, e.g.  
application/x-x509-ca-cert  
in response to the GetCACert operation, DER-encoderd X.509 CA cert)
- Features:
  - Initial Enrolment
  - Renewal (including client key rollover)
  - CA and Client Certificate retrieval
  - CA key and certificate rollover

See also <http://www.ietf.org/proceedings/69/slides/pkix-3.pdf>

# FURTHER READING



Bruce Schneier: Applied Cryptography,  
John Wiley & Sons; 2nd revised edition (16 Nov. 1995)

## Apple Developer Library: Cryptography Concepts In Depth

<https://developer.apple.com/library/content/documentation/Security/Conceptual/cryptoservices/CryptographyConcepts/CryptographyConcepts.html>

## Apple Technical White Paper: 802.1X Authentication

[http://training.apple.com/pdf/WP\\_8021X\\_Authentication.pdf](http://training.apple.com/pdf/WP_8021X_Authentication.pdf)



# THANK YOU!

 <https://github.com/mjung/publications>

**MARKO JUNG**

 [m@mju.ng](mailto:m@mju.ng)

 [@mjung](https://twitter.com/mjung)

 [fb.com/markohjung](https://facebook.com/markohjung)



<http://mju.ng/give>